

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-162950

(43) 公開日 平成7年(1995)6月23日

(51) IntCl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 Q 7/38				
H 0 4 B 1/38				
H 0 4 M 1/00	N	7605-5K	H 0 4 B 7/26	1 0 9 S

審査請求 未請求 請求項の数 11 O L (全 29 頁)

(21) 出願番号 特願平5-302433

(22) 出願日 平成5年(1993)12月2日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 杉谷 俊幸

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

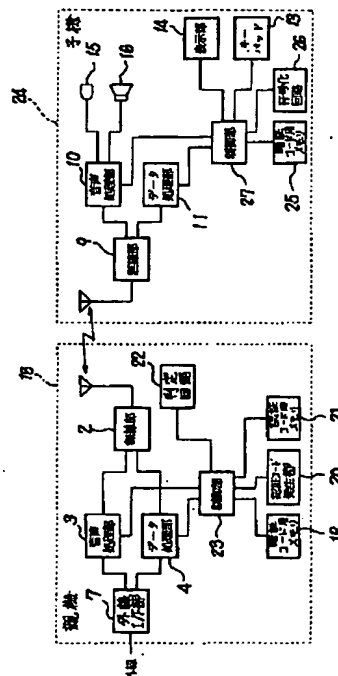
(74) 代理人 弁理士 森本 義弘

(54) 【発明の名称】 無線電話装置

(57) 【要約】

【目的】 IDコードや認証符号が盗聴されても不正使用される危険性を少なくできる無線電話装置を提供することを目的とする。

【構成】 親機18と子機24の双方の暗証コード用メモリ19、25に記憶された暗証コードを利用し、子機24からの通信要求毎に、親機18の認証コード発生部20において任意に生成され送信された認証コードを、これを受信した子機24の符号化回路26で暗証コードと組み合わせ、予め決められた符号化をほどこし認証符号として親機18に対して送信する。親機18の判定回路22において、送信した認証コードと暗証コード用メモリ19に記憶している暗証コードとに基づいて、受信した認証符号が正しく符号化されていると判定して子機24が確認できた場合に、子機24に対して通話を許可する。



【特許請求の範囲】

【請求項 1】 通信網に接続された第 1 の無線装置と、少なくとも 1 つの第 2 の無線装置との間で無線信号を用いて通信を行う無線電話装置であって、前記第 2 の無線装置を、前記第 1 の無線装置が生成し出力した認証コードと、前記第 2 の無線装置に記憶された暗証コードとに基づいて、予め決められた方法で符号化した認証符号を出力するよう構成し、前記第 1 の無線装置を、前記第 1 の無線装置に記憶された暗証コードおよび認証コードに基づいて、前記認証符号の前記符号化の正否を判定し、正しい符号化による認証符号であると判定した場合に、前記第 2 の無線装置に通話を許可するよう構成した無線電話装置。

【請求項 2】 第 1 の無線装置に、暗証コードを記憶する暗証コード記憶部と、適当な認証コードを生成する認証コード発生部と、前記認証コード発生部によって生成された認証コードを記憶する認証コード記憶部と、前記第 1 の無線装置に記憶された暗証コードおよび認証コードに基づいて、第 2 の無線装置から送られる認証符号の符号化の正否を判定する認証符号判定部とを備え、第 2 の無線装置に、前記第 1 の無線装置に記憶された暗証コードと同じ暗証コードを記憶する暗証コード記憶部と、前記第 2 の無線装置に記憶された暗証コードと前記第 1 の無線装置から送られてきた認証コードを組み合わせる予め決められた方法で符号化して前記認証符号を生成する符号化回路とを備え、前記第 1 の無線装置と前記第 2 の無線装置との通話開始の際に、前記第 2 の無線装置は、暗証コードと認証コードの前記組み合わせを少なくとも 1 回行って符号化した前記認証符号を出力し、前記第 1 の無線装置は、前記第 2 の無線装置から出力された前記認証符号が正しい符号化による認証符号であると判定した場合に、前記第 2 の無線装置に通話を許可する請求項 1 に記載の無線電話装置。

【請求項 3】 第 1 の無線装置に、自らが通信を許可した少なくとも 1 つの第 2 の無線装置を識別するための ID コードを記憶する ID コード記憶部と、自らが通信を許可した識別可能な少なくとも 1 つの前記第 2 の無線装置毎に対応して暗証コードを記憶する暗証コード記憶部と、適当な認証コードを生成する認証コード発生部と、前記認証コード発生部によって生成された認証コードを記憶する認証コード記憶部と、前記第 1 の無線装置に記憶された暗証コードおよび認証コードに基づいて、前記第 2 の無線装置から送られる認証符号の符号化の正否を判定する認証符号判定部とを備え、前記第 2 の無線装置に、前記第 1 の無線装置に自らを識別させるための ID コードを記憶する ID コード記憶部と、前記第 1 の無線装置に記憶された自らに対応する暗証コードと同じ暗証コードを記憶する暗証コード記憶部と、前記第 2 の無線装置に記憶された自らに対応する暗証コードと前記第 1 の無線装置から送られてきた認証コードを組み合わせる

予め決められた方法で符号化して前記認証符号を生成する符号化回路とを備え、前記第 1 の無線装置と前記第 2 の無線装置との通話開始の際に、前記第 2 の無線装置は、自らの ID コード記憶部に記憶した ID コードを出力し、前記第 1 の無線装置は、前記第 2 の無線装置から出力された前記 ID コードに基づいて、前記第 2 の無線装置を識別し、さらに、前記第 2 の無線装置は、暗証コードと認証コードの前記組み合わせを少なくとも 1 回行って符号化した前記認証符号を出力し、前記第 1 の無線装置は、前記第 2 の無線装置から出力された前記認証符号が正しい符号化による認証符号であると判定した場合に、前記第 2 の無線装置に通話を許可する請求項 1 に記載の無線電話装置。

【請求項 4】 第 1 の無線装置と第 2 の無線装置の両方に、同一の暗証コードを記憶する書換可能な暗証コード記憶部と、前記暗証コード記憶部に記憶された暗証コードを転送する入出力手段とを備え、前記第 1 の無線装置と前記第 2 の無線装置の少なくとも一方に、前記入出力手段の相互の接続を検知する接続検知手段と、前記接続検知手段からの信号に反応して暗証コードを自動で生成する暗証コード発生部とを備え、第 1 の無線装置と第 2 の無線装置の前記入出力手段の相互接続の際に、前記入出力手段を介して、第 1 の無線装置および第 2 の無線装置の前記暗証コード記憶部の内容を、前記暗証コード発生部が生成した暗証コードに書き換え、この暗証コードを利用して前記第 1 の無線装置が前記第 2 の無線装置を識別する請求項 1 に記載の無線電話装置。

【請求項 5】 第 1 の無線装置と第 2 の無線装置の両方に、同一の暗証コードを記憶する書換可能な暗証コード記憶部と、前記暗証コード記憶部に記憶された暗証コードを転送する入出力手段とを備え、前記第 1 の無線装置と前記第 2 の無線装置の少なくとも一方に、前記入出力手段の相互の接続を検知する接続検知手段と、暗証コードを自動で生成する暗証コード発生部と、前記接続検知手段からの信号に反応して、前記入出力手段を介して送られてきた暗証コードが自らの前記暗証コード記憶部に記憶された暗証コードと同一であると判定し場合に、前記暗証コード発生部を起動し、前記入出力手段を介して、第 1 の無線装置および第 2 の無線装置の前記暗証コード記憶部の内容を、前記暗証コード発生部が生成した暗証コードに書き換える制御部とを備え、前記制御部により書き換えられた前記暗証コードを利用して前記第 1 の無線装置が前記第 2 の無線装置を識別する請求項 1 に記載の無線電話装置。

【請求項 6】 第 1 の無線装置と第 2 の無線装置の両方に、同一の暗証コードを記憶する書換可能な暗証コード記憶部とを備え、前記第 1 の無線装置と前記第 2 の無線装置の少なくとも一方に、第 1 の無線装置および第 2 の無線装置の前記暗証コード記憶部を、自動で生成した暗証コードに書き換える暗証コード発生部と、前記暗証コ

ード発生部で生成された暗証コードを、前記暗証コード記憶部の前記書き換えの前の暗証コードにより予め決められた方法で暗号化する暗号化部と、前記暗号化部で暗号化された暗証コードを変調し無線信号として出力する送信部とを備え、前記第1の無線装置と前記第2の無線装置の両方、または、前記第1の無線装置と前記第2の無線装置のうちで、前記暗証コード発生部と前記暗号化部と前記送信部とが備えられていない方に、前記暗号化部で暗号化された暗証コードを、前記無線信号から復調して取り出す受信部と、前記受信部で取り出された暗号化された前記暗証コードを、前記暗証コード記憶部の前記書き換えの前の暗証コードにより復号し、前記暗証コード記憶部の前記書き換えの前の暗証コードを更新する復号部とを備え、前記復号部により更新された暗証コードを利用して前記第1の無線装置が前記第2の無線装置を識別する請求項1に記載の無線電話装置。

【請求項7】 第1の無線装置に、暗証コードを記憶する暗証コード記憶部と、通信要求のあった他の無線装置の確認の際に、不正な無線装置と判断し通信を拒否した回数をカウントする計数部と、通信拒否状態になったときに通常の状態に復帰するためのリセット信号を入力する入力手段とを備え、前記計数部でカウントされる通信拒否の回数が、予め決められた回数に達すると、前記入力手段からリセット信号が入力され、前記計数部のカウントがクリアされるまで他の全ての無線装置からの通信要求を拒否し、前記第1の無線装置に記憶された暗証コードを利用して前記第1の無線装置が前記第2の無線装置を識別する請求項1に記載の無線電話装置。

【請求項8】 第1の無線装置に、自らが通信を許可した少なくとも1つの第2の無線装置を識別するためのIDコードを記憶するIDコード記憶部と、自らが通信を許可した識別可能な少なくとも1つの前記第2の無線装置毎に対応して暗証コードを記憶する暗証コード記憶部と、通信要求のあった他の無線装置の確認の際に不正な無線装置と判断し通信を拒否した回数を通信が許可されたIDコードをもつ第2の無線装置ごとにカウントし記憶する計数部と、通信拒否状態になったときに通常の状態に復帰するためのリセット信号を入力する入力手段とを備え、前記計数部でカウントされる通信が許可された第2の無線装置ごとの通信拒否の回数が、予め決められた回数に達すると、前記入力手段からリセット信号が入力され、前記計数部のカウントがクリアされるまで該当するIDコードをもつ前記第2の無線装置からの通信要求を拒否する請求項1に記載の無線電話装置。

【請求項9】 第1の無線装置に、複数の暗証コードを記憶する暗証コード記憶部と、任意に1つの暗証コードを選び出し、どの暗証コードを利用して符号化させるかを指定する暗証コード選択部と、適当な認証コードを生成する認証コード発生部と、前記認証コード発生部によって生成された認証コードを記憶する認証コード記憶部

と、前記暗証コード選択部によって選ばれた暗証コードおよび前記認証コード記憶部に記憶された認証コードに基づいて、第2の無線装置から送られる認証符号の符号化の正否を判定する認証符号判定部とを備え、第2の無線装置に、前記第1の無線装置に記憶された複数の暗証コードと同じ暗証コードを記憶する暗証コード記憶部と、前記第2の無線装置に記憶された暗証コードのうちから前記暗証コード選択部により選択された暗証コードと同じ暗証コードを選び出し、この暗証コードと前記第1の無線装置から送られてきた認証コードを組み合わせ、指定された暗証コード毎に予め決められた方法で符号化して前記認証符号を生成する符号化回路とを備え、前記第1の無線装置と前記第2の無線装置との通話開始の際に、前記第2の無線装置は、暗証コードと認証コードの前記組み合わせを少なくとも1回行って符号化した前記認証符号を出力し、前記第1の無線装置は、前記第2の無線装置から出力された前記認証符号が正しい符号化による認証符号であると判定した場合に、前記第2の無線装置に通話を許可する請求項1に記載の無線電話装置。

【請求項10】 第1の無線装置に、複数の暗証コードを記憶する暗証コード記憶部と、任意に少なくとも1つの暗証コードを選び出し、どの暗証コードを利用して符号化させるかを指定する暗証コード選択部と、適当な認証コードを生成する認証コード発生部と、前記認証コード発生部によって生成された認証コードを記憶する認証コード記憶部と、前記暗証コード選択部によって選ばれた暗証コードおよび前記認証コード記憶部に記憶された認証コードに基づいて、第2の無線装置から送られる認証符号の符号化の正否を判定する認証符号判定部とを備え、第2の無線装置に、前記第1の無線装置に記憶された複数の暗証コードと同じ暗証コードを記憶する暗証コード記憶部と、前記第2の無線装置に記憶された暗証コードのうちから前記暗証コード選択部により選択された全ての暗証コードと同じ暗証コードを選び出し、これらの各暗証コードと前記第1の無線装置から送られてきた認証コードを組み合わせ、指定された暗証コード毎に予め決められた方法で符号化して前記認証符号を生成する符号化回路とを備え、前記第1の無線装置と前記第2の無線装置との通話開始の際に、前記第2の無線装置は、暗証コードと認証コードの前記組み合わせを少なくとも1回行って符号化した前記認証符号を出力し、前記第1の無線装置は、前記第2の無線装置から出力された前記認証符号が正しい符号化による認証符号であると判定した場合に、前記第2の無線装置に通話を許可する請求項1に記載の無線電話装置。

【請求項11】 第1の無線装置に、複数の暗証コードを記憶する暗証コード記憶部と、任意に少なくとも1つの暗証コードを選び出し、どの暗証コードを利用して符号化させるかを指定する暗証コードを選択部と、適当な

認証コードを生成する認証コード発生部と、前記認証コード発生部によって生成された認証コードを記憶する認証コード記憶部と、前記暗証コード選択部によって選ばれた暗証コードおよび前記認証コード記憶部に記憶された認証コードに基づいて、第2の無線装置から送られる認証符号の符号化の正否を判定する認証符号判定部とを備え、第2の無線装置に、前記第1の無線装置に記憶された複数の暗証コードと同じ暗証コードを記憶する暗証コード記憶部と、前記第2の無線装置に記憶された暗証コードのうちから前記暗証コード選択部により選択された全ての暗証コードと同じ暗証コードを選び出し、これらの全ての暗証コードと前記第1の無線装置から送られてきた認証コードを組み合わせて、予め決められた方法で符号化して前記認証符号を生成する符号化回路とを備え、前記第1の無線装置と前記第2の無線装置との通話開始の際に、前記第2の無線装置は、暗証コードと認証コードの前記組み合わせを少なくとも1回行って符号化した前記認証符号を出力し、前記第1の無線装置は、前記第2の無線装置から出力された前記認証符号が正しい符号化による認証符号であると判定した場合に、前記第2の無線装置に通話を許可する請求項1に記載の無線電話装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、公衆基地局または親機と、これらと無線回線を利用して通信可能な子機とから構成される無線電話装置に関するものである。

【0002】

【従来の技術】近年、コードレス電話や自動車電話などの無線を利用した無線電話装置の発展がめざましく利用者の数が増大している。

【0003】以下、図面を参照しながら従来の無線電話装置の説明を行う。図17は従来の無線電話装置の構成を示すブロック図である。図17において、1は親機であり、2は信号の送受信および変復調を行う無線部、3はエキスパンダー、コンパンダー、コンプレッサーなどからなる音声信号の処理を行う音声処理部、4はダイヤルディジット信号やIDコードやリンク確立要求などの子機からの制御データなどの処理や子機の呼出信号の生成を行うデータ処理部、5は親機1と通話が許可されている子機のIDコードが記憶されているIDコード用メモリ、6は親機1全体の制御を行う制御部、7は外線との音声信号や着呼信号などのやりとりを行う外線インターフェイス部（外線I/F部）である。

【0004】また、8は子機であり、9は信号の送受信および変復調を行う無線部、10はエキスパンダー、コンパンダー、コンプレッサーなどからなる音声信号の処理を行う音声処理部、11はダイヤルディジット信号や通話チャンネル指定信号などの親機1からの制御データなどの処理や親機1の呼出信号の生成を行うデータ処理

部、12は子機8のIDコードが記憶されているIDコード用メモリ、13は通話要求やダイヤル情報などを入力するキーパッド、14は入力されたダイヤル情報などを表示する表示部、15は音声の入力を行うマイク、16は音声の出力を行うスピーカ、17は子機8全体の制御を行う制御部である。

【0005】図18は、子機8から親機1への通話要求があったときの信号のやり取りのシーケンスの例を示す図である。以上のように構成されたコードレス電話についてその動作を説明する。子機8より電話をかける場合、使用者はまず始めにキーパッド13に設けられた発呼ボタンを押す。制御部17は、発呼ボタンが押されたことを検知すると、データ処理部11にリンク確立要求を生成させるための制御信号を出力する。データ処理部11では、制御信号にしたがってリンク確立要求の信号を生成し、無線部9に出力し、無線部9で無線信号が生成され出力される。一方、親機1の無線部2は、常に制御チャンネルのスキャンを行っており、子機8からの無線信号を受信すると、その復調信号がデータ処理部4に伝えられる。データ処理部4では復調信号を解析し受信した制御信号の情報を制御部6に出力する。上記のように子機8よりリンク確立要求が出されると、子機8からの信号は、データ処理部4にて検知され制御部6に伝えられる。制御部6ではリンク確立要求が受信されたことが伝えられると、リンク確立のシーケンスを起動し、ID要求の信号を生成し出力するようにデータ処理部4を制御する。データ処理部4では、制御信号にしたがってID要求の信号を生成し、無線部2に出力し、無線部2で無線信号が生成され出力される。このとき、子機8はリンク確立要求を出力したあと親機1からの応答待ち状態になっている。親機1がID要求信号を送信すると、無線部9で受信され、復調信号がデータ処理部11に出力される。そしてID要求信号が受信されたことが制御部17に伝えられる。制御部17では、IDコード用メモリ12より自らのIDコードを読みだし、IDコードの送信、すなわちID応答の出力シーケンスを開始し、上記リンク確立要求の出力の場合と同様にデータ処理部11、無線部9が動作し、IDコードが親機1に出力される。親機1では、上記リンク確立要求受信の場合と同様にして、子機8より送信されたIDコードが受信され制御部6に伝えられる。制御部6では、登録された子機のIDコードが記憶されたIDコード用メモリ5を検索し、受信したIDコードが、登録された子機8のものであるか否かを確認する。受信したIDコードが登録されている場合は、正当な子機8からの通信であると判断され、ID認可の応答を出力し、親機子機間のリンクが確立され、通話チャンネルの指定などのシーケンスを経て、親機子機間が通話状態に至る。また、受信したIDコードが登録されていなかった場合は、不当な子機からの通信であると判断され、通信が拒否される。

【0006】次に図18を用いて、従来の無線電話装置の親機子機間での通話要求からリンク確立までにやり取りされる信号の流れを説明する。図に示すように子機8では、使用者が発呼ボタンを押して電話をかけようとすると、まず、親機1にリンクの確立を要求するリンク確立要求が出力される。親機1からは、子機8の確認のためにIDコードを要求するID要求が出力され、子機8では、それに応答して自らのIDコードを出力する。親機1は、子機8からのIDコードを受け取ると、受け取ったIDコードと登録された子機のIDコードを比較し、一致するものがあれば、ID認可を出力し、通話チャネルの指定などのシーケンスを経て、親機子機間の通話が開始される。

【0007】

【発明が解決しようとする課題】しかしながら、上記のような従来の無線電話装置では、子機の確認がIDコードのみで行われていたため、IDコードを盗聴し、他人の無線電話装置の親機を使用して電話をかけたり、セルラー電話においても他人のIDコードを利用して電話をかけるという不正使用が行われるという問題点を有していた。

【0008】本発明は、上記従来の問題点を解決するもので、子機が通信要求の際に送信するIDコードや認証符号が盗聴されても、不正使用される危険性を少なくできる無線電話装置を提供することを目的としている。

【0009】

【課題を解決するための手段】上記課題を解決するために本発明の無線電話装置は、通信網に接続された第1の無線装置と、少なくとも1つの第2の無線装置との間で無線信号を用いて通信を行う無線電話装置であって、前記第2の無線装置を、前記第1の無線装置が生成し出力した認証コードと、前記第2の無線装置に記憶された暗証コードとに基づいて、予め決められた方法で符号化した認証符号を出力するよう構成し、前記第1の無線装置を、前記第1の無線装置に記憶された暗証コードおよび認証コードに基づいて、前記認証符号の前記符号化の正否を判定し、正しい符号化による認証符号であると判定した場合に、前記第2の無線装置に通話を許可する構成とする。

【0010】

【作用】上記の構成によると、第1の無線装置と第2の無線装置の双方に記憶された暗証コードを利用し、第2の無線装置からの通信要求毎に、第1の無線装置において任意に生成され送信された認証コードを、第2の無線装置で暗証コードと組み合わせ、予め決められた符号化をほどこし認証符号として第1の無線装置に対して送信する。

【0011】第1の無線装置において、送信した認証コードと記憶している暗証コードとに基づいて、受信した認証符号が正しく符号化されていると判定して第2の無

線装置が確認できた場合に、第2の無線装置に対して通話を許可する。

【0012】

【実施例】以下、本発明の実施例について、図面を参照しながら説明する。なお、従来例と同様の作用効果を奏するものには同一の符号を付してその説明を省略する。

【0013】図1は本発明の第1の実施例を示す無線電話装置のブロック図である。図1において、18は第1の無線装置としての親機であり、19は子機によって設定された暗証コードを記憶する暗証コード記憶部としての暗証コード用メモリ、20は認証コードを生成する認証コード発生部、21は認証コード発生部20で作られた認証コードを記憶する認証コード記憶部としての認証コード用メモリ、22は子機より送られてくる認証符号の判定を行う認証符号判定部としての判定回路、23は親機18全体の制御を行う制御部である。

【0014】また、24は第2の無線装置としての子機であり、25は暗証コードが記憶された暗証コード記憶部としての暗証コード用メモリ、26は親機18から送られてきた認証コードと暗証コードを組み合わせ、あらかじめ決められた方法で変換する符号化をほどこし認証符号を生成する符号化回路、27は子機24全体の制御を行う制御部である。

【0015】図2は、子機24から親機18への通話要求があったときの信号のやり取りのシーケンスの例を示す図である。以上のように構成された無線電話装置についてその動作を説明する。子機24のキーパッド13の発呼ボタンが押されると、リンク確立要求が子機24より出力される。親機18が子機24から出されたリンク確立要求を受信すると、認証コードと暗証コードを用いて子機の確認が行われる。まず、親機18の認証コード発生部20で、ランダムなコードが生成され、認証コードとして認証コード用メモリ21に記憶される。このとき生成された認証コードは無線信号を利用して子機24に伝えられる。子機24では、認証コードを受け取ると、そのコードが符号化回路26に伝えられる。また、符号化回路26には暗証コード記憶用メモリ25に記憶された暗証コードも伝えられる。符号化回路26では認証コードと暗証コードを組み合わせ、あらかじめ決められた方法で変換する符号化をほどこし認証符号を生成する。子機24はこの認証符号を親機18に送信し、親機18では受信した認証符号を判定回路22に伝える。判定回路22では暗証コード用メモリ19および認証コード用メモリ21に記憶された暗証コードと認証コードをもとに、子機24より送られてきた認証符号が正しく符号化されているかを判定し、制御部23に出力する。制御部23では、受信した認証符号が正しく符号化されている場合は、正当な子機からの通信であると判断し、親機子機間のリンクを確立し、通話チャネルの指定などのシーケンスを経て、親機子機間を通話状態にするように

制御を行う。また、受信した認証符号正しくなかった場合は、不当な子機からの通信であると判断し、通信を拒否する。

【0016】次に図2を用いて、本発明の一実施例である図1に示す無線電話装置の親機子機間での通話要求からリンク確立までにやり取りされる信号の流れを説明する。図に示すように子機では、使用者が発呼ボタンを押して電話をかけようとする、まず、親機にリンクの確立を要求するリンク確立要求が出力される。リンク確立要求を受け取った親機からは、認証コード発生部で生成された認証コードを子機に出力する。子機は、送られてきた認証コードと暗証コードを組み合わせて符号化回路で符号化し、親機に出力する。親機では、子機より送られてきた認証符号が正しく符号化されているかを判定し、正しく符号化されている場合は、リンクが確立し、通話チャネルの指定などを経て通話モードにはいる。又、子機から送られてきた認証符号が正しく符号化されていない場合は、その時点で通信が拒否され、リンクは確立されない。なお、本実施例では、符号化の一例として認証コードと暗証コードの論理積をとって認証符号とする例を示しており、図2に示すように、親機から送られてくる認証コードが01011011、暗証コードが11010001である場合、正しく符号化された認証符号は、01010001となり、子機はこの01010001を認証符号として親機に送信している。

【0017】次に第2の実施例について説明を行う。図3は本発明の第2の実施例を示す無線電話装置のブロック図である。上記した従来例、実施例と同様の効果、作用を有するものには、同一の番号を付し、説明を省略する。図3において、28は3台の子機が登録可能な第1の無線装置としての親機であり、20は認証コードを生成する認証コード発生部、21は認証コード発生部20で作られた認証コードを記憶する認証コード記憶部としての認証コード用メモリ、22は子機より送られてくる認証符号の判定を行う認証符号判定部としての判定回路、29は親機28に登録された3台の子機のIDコードがそれぞれ記憶されたIDコード記憶部としてのIDコード用メモリ、30は登録された3台の子機の各々の暗証コードが記憶された暗証コード記憶部としての暗証コード用メモリ、31は親機28全体の制御を行う制御部である。

【0018】また、32は第2の無線装置としての子機であり、25は暗証コードが記憶された暗証コード記憶部としての暗証コード用メモリ、26は親機28から送られてきた認証コードと暗証コードを組み合わせて、あらかじめ決められた方法で変換する符号化をほどこし認証符号を生成する符号化回路、33は子機32全体の制御を行う制御部である。なお、12は、従来例と同様に自らのIDコードを記憶したIDコード記憶部としてのIDコード用メモリである。

【0019】図4は、子機32から親機28への通話要求があったときの信号のやり取りのシーケンスの例を示す図である。以上のように構成された無線電話装置についてその動作を説明する。子機32のキーパッド13の発呼ボタンが押されると、リンク確立要求が子機32より出力される。親機28が子機32から出されたリンク確立要求を受信すると、子機32に対しID要求を出力する。ID要求を受信した子機32の制御部33は、IDコード用メモリ12より、IDコードを読みだし、親機28に出力する。子機32からのIDコードを受信した親機28の制御部31は、IDコード用メモリ29を検索し、どの子機からの通話要求であるかを調べる。続いて、認証コードと暗証コードを用いて子機の再確認が行われる。親機28の認証コード発生部20で、ランダムなコードが生成され、認証コードとして認証コード用メモリ21に記憶される。このとき生成された認証コードは無線信号を利用して子機32に伝えられる。子機32では、認証コードを受け取ると、そのコードが符号化回路26に伝えられる。また、符号化回路26には暗証コード記憶用メモリ25に記憶された暗証コードも伝えられる。符号化回路26では認証コードと暗証コードを組み合わせて、あらかじめ決められた方法で変換する符号化をほどこし認証符号を生成する。子機32はこの認証符号を親機28に送信する。親機28の制御部31は、受信した認証符号と認証コード用メモリ21に記憶されている認証コードを判定回路22に伝え、また、暗証コード用メモリ30より該当する子機の暗証コードを読みだし判定回路22に伝える。判定回路22では制御部31より受け取った暗証コードと認証コードをもとに、認証符号が正しく符号化されているかを判定し、制御部31に出力する。制御部31では、受信した認証符号が正しく符号化されている場合は、正当な子機からの通信であると判断し、親機子機間のリンクを確立し、通話チャネルの指定などのシーケンスを経て、親機子機間が通話状態にするように制御を行う。また、受信した認証符号正しくなかった場合は、不当な子機からの通信であると判断し、通信を拒否する。

【0020】次に図4を用いて、本発明の第2の実施例である図3に示す無線電話装置の親機子機間での通話要求からリンク確立までにやり取りされる信号の流れを説明する。図に示すように子機では、使用者が発呼ボタンを押して電話をかけようとする、まず、親機にリンクの確立を要求するリンク確立要求が出力される。リンク確立要求を受け取った親機からは、ID要求の信号が出力され、子機は、IDコードを出力する。子機からのIDコードを受け取った親機は、受け取ったIDコードが登録されたいずれかの子機のIDコードと一致するかを調べ、一致するものがあれば、認証コード発生部で生成された認証コードを子機に出力する。一致するIDコードが無かった場合は、ここで通話が拒否される。子機

は、親機から認証コードが送られてくると、送られてきた認証コードと暗証コードを組み合わせて符号化回路で符号化し、親機に出力する。親機では、子機より送られてきた認証符号が正しく符号化されているかを判定し、正しく符号化されている場合は、リンクが確立し、通話チャネルの指定などを経て通話モードにはいる。又、子機から送られてきた認証符号が正しく符号化されていない場合は、その時点で通信が拒否され、リンクは確立されない。なお、本実施例では、登録された子機の内1台の子機の暗証コードが11010001であり、符号化の一例として認証コードと暗証コードの論理積をとって認証符号とする例を示しており、図4に示すように、親機から送られてくる認証コードが01011011、暗証コードが11010001である場合、正しく符号化された認証符号は、01010001となり、子機はこの01010001を認証符号として親機に送信している。

【0021】次に第3の実施例について説明を行う。図5は本発明の第3の実施例を示す無線電話装置のブロック図である。上記した従来例、実施例と同様の効果、作用を有するものには、同一の図番を付し、説明を省略する。

【0022】図5において、34は第1の無線装置としての親機であり、20は認証コードを生成する認証コード発生部、21は認証コード発生部20で作られた認証コードを記憶する認証コード記憶部としての認証コード用メモリ、22は子機より送られてくる認証符号の判定を行う認証符号判定部としての判定回路、35は暗証コードを記憶する書換可能な暗証コード記憶部としての暗証コード用メモリ、36は暗証コードを生成する暗証コード発生部、37は暗証コードのやり取りを行う入出力手段としてのインターフェイス部(I/F部)、38はインターフェイス部37が外部と接続されたことを検知する接続検知手段としての接続検知部、39は親機34全体の制御を行う制御部である。

【0023】また、40は第2の無線装置としての子機であり、26は親機34から送られてきた認証コードと暗証コードを読み合わせて、あらかじめ決められた方法で変換する符号化をほどこし認証符号を生成する符号化回路、41は暗証コードが記憶された書換可能な暗証コード記憶部としての暗証コード用メモリ、42は暗証コードのやり取りを行う入出力手段としてのインターフェイス部(I/F部)、43は子機40全体の制御を行う制御部である。

【0024】上記のように構成された親機34と子機40から構成される無線電話装置において、通話要求から通話にいたる動作は、上記した図1に示す第1の実施例と同様であり説明を省略する。ここでは、親機34のインターフェイス部37と子機40のインターフェイス部42が接続され各々の暗証コードが書き換えられる際の

動作について説明を行う。

【0025】親機34のインターフェイス部37と子機40のインターフェイス部42が接続されると、接続検知部38より検知信号が暗証コード発生部36に伝えられる。暗証コード発生部36は、検知信号が伝えられると、あらかじめ決められた桁数の暗証コードをランダムに作り制御部39に出力する。制御部39では、暗証コード発生部36で作られた新しい暗証コードをインターフェイス部37を介して子機40に出力するとともに、暗証コード用メモリ35の内容を新しい暗証コードに書き換える。子機40では、親機34から出力された新しい暗証コードは、インターフェイス部42を介して制御部43に伝えられる。制御部43は、新しい暗証コードを受け取ると暗証コード用メモリ41の内容を新しい暗証コードに書き換える。

【0026】次に第4の実施例について説明を行う。図6は本発明の第4の実施例を示す無線電話装置のブロック図である。上記した従来例、実施例と同様の効果、作用を有するものには、同一の図番を付し、説明を省略する。

【0027】図6において、44は第1の無線装置としての親機であり、20は認証コードを生成する認証コード発生部、21は認証コード発生部20で作られた認証コードを記憶する認証コード記憶部としての認証コード用メモリ、22は子機より送られてくる認証符号の判定を行う認証符号判定部としての判定回路、35は暗証コードを記憶する書換可能な暗証コード記憶部としての暗証コード用メモリ、36は暗証コードを生成する暗証コード発生部、37は暗証コードなどのやり取りを行う入出力手段としてのインターフェイス部(I/F部)、45はインターフェイス部37が外部と接続されたことを検知する接続検知手段としての接続検知部、46は子機から送られてきた暗証コードが暗証コード用メモリ35に記憶されている暗証コードと同じであるか否かを判定する暗証コード判定器、47は親機44全体の制御を行う制御部である。

【0028】また、48は第2の無線装置としての子機であり、26は親機44から送られてきた認証コードと暗証コードを読み合わせて、あらかじめ決められた方法で変換する符号化をほどこし認証符号を生成する符号化回路、41は暗証コードが記憶された書換可能な暗証コード記憶部としての暗証コード用メモリ、42は暗証コードのやり取りを行う入出力手段としてのインターフェイス部(I/F部)、49は子機48全体の制御を行う制御部である。

【0029】上記のように構成された親機44と子機48から構成される無線電話装置において、通話要求から通話にいたる動作は、上記した図1に示す第1の実施例と同様であり説明を省略する。ここでは、親機44のインターフェイス部37と子機48のインターフェイス部

42が接続され各々の暗証コードが書き換えられる際の動作について説明を行う。

【0030】親機44のインターフェイス部37と子機48のインターフェイス部42が接続されると、接続検知部45より検知信号が制御部47に伝えられる。制御部47では、検知信号が伝えられると、インターフェイス部37を介して、子機に暗証コードの出力要求を行う。暗証コードの出力要求は、子機48のインターフェイス部42を介して制御部49に伝えられる。制御部49は、出力要求を受け取ると、暗証コード用メモリ41より暗証コードを読みだし、インターフェイス部42を介して親機に出力する。親機44の制御部47は、子機からの暗証コードをインターフェイス37を介し受け取り、暗証コード判定器46に出力する。また、制御部47は、暗証コード用メモリ35に記憶された暗証コードを読みだし暗証コード判定器46に出力する。暗証コード判定器46は、子機から送られてきた暗証コードと暗証コード用メモリ35に記憶されている暗証コードが同じであるか否かを判定し、制御部47に出力する。制御部47は、各々の暗証コードが一致すれば、暗証コード発生部36を起動する。暗証コード発生部36は、制御部47によって起動されると、あらかじめ決められた桁数の暗証コードをランダムに作り制御部47に出力する。制御部47では、暗証コード発生部36で作られた新しい暗証コードをインターフェイス部37を介して子機48に出力するとともに、暗証コード用メモリ35の内容を新しい暗証コードに書き換える。子機48では、親機44から出力された新しい暗証コードが、インターフェイス部42を介して制御部49に伝えられる。制御部49は、新しい暗証コードを受け取ると暗証コード用メモリ41の内容を新しい暗証コードに書き換える。

【0031】次に第5の実施例について説明を行う。図7は本発明の第5の実施例を示す無線電話装置のブロック図である。上記した従来例、実施例と同様の効果、作用を有するものには、同一の図番を付し、説明を省略する。

【0032】図7において、50は第1の無線装置としての親機であり、20は認証コードを生成する認証コード発生部、21は認証コード発生部20で作られた認証コードを記憶する認証コード記憶部としての認証コード用メモリ、22は子機より送られてくる認証符号の判定を行う認証符号判定部としての判定回路、35は暗証コードを記憶する書換可能な暗証コード記憶部としての暗証コード用メモリ、36は暗証コードを生成する暗証コード発生部、51は無線の信号を受信し復調する受信部、52は音声やデータなどを変調し無線信号を生成する送信部、53は暗証コードを暗号化する暗号化部としての暗証コード暗号化器、54は親機50全体の制御を行う制御部である。

【0033】また、55は第2の無線装置としての子機

であり、26は親機50から送られてきた認証コードと暗証コードを組み合わせ、あらかじめ決められた方法で変換する符号化をほどこし認証符号を生成する符号化回路、41は暗証コードが記憶された書換可能な暗証コード記憶部としての暗証コード用メモリ、56は無線の信号を受信し復調する受信部、57は音声やデータなどを変調し無線信号を生成する送信部、58は暗号化された暗証コードを復号しもとの暗証コードに戻す復号部としての暗証コード復号器、59は子機55全体の制御を行う制御部である。

【0034】図8は、子機55から親機50への通話要求があり、暗証コードの書き換えが行われるとき信号のやり取りのシーケンスの例を示す図である。以上のように構成された無線電話装置についてその動作を説明する。子機55のキーパッド13の発呼ボタンが押されると、リンク確立要求が子機55より出力される。親機50が子機55から出されたリンク確立要求を受信すると、親機50の制御部は、認証コード発生部20を起動し、認証コード発生部20で、ランダムなコードが生成され、制御部54に出力される。制御部54に送られた認証コードは、認証コード用メモリ21に記憶される。また、親機50の制御部54は、データ処理部4を起動しこの認証コードを出力し、データ処理部4では、認証コードを送信部52に伝え、認証コードが無線信号として子機55に出力される。子機55では、認証コードを受け取ると、そのコードが符号化回路26に伝えられる。また、符号化回路26には暗証コード記憶用メモリ41に記憶された暗証コードも伝えられる。符号化回路26では認証コードと暗証コードを組み合わせ、あらかじめ決められた方法で変換する符号化をほどこし認証符号を生成する。子機55の制御部59は、データ処理部11を起動しこの認証符号を出力し、データ処理部11では、認証符号を送信部57に伝え、認証符号が無線信号として親機50に出力される。親機50では、子機55からの認証符号が、受信部51で復調され、データ処理部4に送られる。データ処理部4は、認証符号を制御部54に伝える。制御部54は認証符号を受け取ると、その認証符号を判定回路22に伝える。又、制御部54は認証コード用メモリ21に記憶された認証コードと、暗証コード用メモリ35に記憶された暗証コードを読みだし判定回路22に伝える。判定回路22では暗証コード用メモリ35および認証コード用メモリ21に記憶された暗証コードと認証コードをもとに、子機55より送られてきた認証符号が正しく符号化されているかを判定し、制御部54に出力する。制御部54では、受信した認証符号が正しく符号化されている場合は、正当な子機からの通信であると判断し、暗証コード発生部36を起動する。暗証コード発生部36は、制御部54によって起動されると、あらかじめ決められた桁数の暗証コードをランダムに作り制御部54に出力する。制御部54で

は、前もって暗証コード用メモリ35より読み出された暗証コードと暗証コード発生部36で作られた新しい暗証コードを暗証コード暗号化器53に出力し、暗証コード暗号化器は、暗証コード発生部36で作られた暗証コードと暗証コード用メモリ35に記憶されていた暗証コードとを組み合わせるあらかじめ決められた方法で暗号化し、制御部54に出力する。制御部54では、暗号化された暗証コードをデータ処理部4に出力する。データ処理部4では、暗号化された暗証コードを無線信号として出力するためのデータ処理を行い、送信部52に出力し、送信部52より暗号化された暗証コードが無線の信号として子機55に出力される。子機55では、受信部56にて暗号化された暗証コードが受信されると、データ処理部11に伝えられ、データ処理部11から、制御部59に伝えられる。制御部59では、受け取った暗号化された暗証コードを暗証コード復号器58に出力する。又、制御部59は、先に読み込んだ暗証コード用メモリ41に記憶されていた暗証コードを暗証コード復号器58に出力する。暗証コード復号器58では、親機より送られてきた暗号化された暗証コードを暗証コード用メモリに記憶されていた暗証コードを用いてあらかじめ決められた方法で親機50の暗証コード発生部36で作られた新しい暗証コードに復号し、制御部59に出力する。制御部59は、暗証コード復号器58にて復号された新しい暗証コードを暗証コード用メモリ41に出力し暗証コード用メモリ41の内容を更新する。また、制御部59は、新しい暗証コードを受信したことを親機に知らせる新暗証コード受信確認信号を出力するようにデータ処理部11を制御し、データ処理部11で新暗証コード受信確認信号が作られ、送信部57に伝えられ、無線信号として親機50に出力される。親機50の受信部51にて子機からの新暗証コード受信確認信号が受信され、データ処理部4に伝えられると、データ処理部4は、制御部54に子機が新暗証コードを受信したことを知らせる信号を出力し、制御部54は、先に暗証コード発生部36にて作られた新暗証コードを暗証コード用メモリ35に出力し、暗証コード用メモリ35の内容を更新する。

【0035】次に図8を用いて、本発明の第5の実施例である図7に示す無線電話装置の親機子機間での通話要求からリンク確立までにやり取りされる信号の流れを説明する。図に示すように子機では、使用者が発呼ボタンを押して電話をかけようとする、まず、親機にリンクの確立を要求するリンク確立要求が出力される。リンク確立要求を受け取った親機は、認証コード発生部で生成された認証コードを子機に出力する。子機は送られてきた認証コードと暗証コードを組み合わせ符号化回路で符号化し、親機に出力する。親機は子機より送られてきた認証符号が正しく符号化されているかを判定し、正しく符号化されている場合は、暗証コードの書換のシーケ

スを開始し、新しい暗証コードと旧暗証コードを組み合わせるで作られた暗号化された新暗証コードを子機に出力する。子機は、受け取った暗号化された新暗証コードを旧暗証コードを用いて復号し暗証コードを更新するとともに、新暗証コード受信確認信号を出力する。親機は、新暗証コード受信確認信号を受け取ると、自らの暗証コードを更新する。その後、通話チャネルの指定などのシーケンスを経て通常の通話モードに進む。

【0036】なお、本実施例では、認証コードの符号化の一例として認証コードと暗証コードの論理積をとって認証符号とする例を示しており、図8に示すように、親機から送られてくる認証コードが01011011、暗証コードが11010001である場合、正しく符号化された認証符号は、01010001となり、子機はこの01010001を認証符号として親機に送信している。また、暗証コードの暗号化の例として、本実施例では、旧暗証コードと、新暗証コードの和をとることにより暗号化する方法を示しており、親機子機それぞれにあらかじめ記憶されていた旧暗証コードが上記のように11010001、新しく作られた暗証コードが01011001である場合、親機からは、暗号化された暗証コードとして、それぞれの和である100101010が子機に送られる。また、暗号化された暗証コード100101010を受け取った子機は、その値より、旧暗証コード11010001を引いて新暗証コード01011001を復号している。

【0037】図9は本発明の第6の実施例を示す無線電話装置のブロック図である。図9において、60は第1の無線装置としての親機であり、19は子機によって設定された暗証コードを記憶する暗証コード記憶部としての暗証コード用メモリ、20は認証コードを生成する認証コード発生部、21は認証コード発生部20で作られた認証コードを記憶する認証コード記憶部としての認証コード用メモリ、22は子機より送られてくる認証符号の判定を行う認証符号判定部としての判定回路、61は不正な子機からの通話要求の回数をカウントする計数部としてのカウンター、62は通話拒否の状態になったときに通常の状態に戻すための入力手段としてのリセットボタン、63は親機60全体の制御を行う制御部である。

【0038】また、24は第2の無線装置としての子機であり、25は暗証コードが記憶された暗証コード記憶部としての暗証コード用メモリ、26は親機60から送られてきた認証コードと暗証コードを組み合わせ、あらかじめ決められた方法で変換する符号化を施し認証符号を生成する符号化回路、27は子機24全体の制御を行う制御部である。

【0039】以上のように構成された無線電話装置についてその動作を説明する。なお、同一の暗証コードを有する正当な子機からの通話要求から通話状態にいたる親

機 60 の動作は、図 1 に示した第 1 の実施例と同一であり説明を省略し、不正な子機からの通話要求があったときの動作について説明を行う。

【0040】本説明では、子機 24 は不正な子機であるとし、暗証コード用メモリに記憶されて暗証コードは、親機の暗証コードとことなる 11001100 が記憶されているものとする。子機 24 から通話要求を行う場合、使用者は、子機 24 のキーパッド 13 の発呼ボタンを押し、リンク確立要求を出力する。親機 60 は、子機 24 から出されたリンク確立要求を受信すると、認証コードと暗証コードを用いて子機の確認をおこなう。図 1 に示した第 1 の実施例と同様に、親機 60 の認証コード発生部 20 で、ランダムなコードが生成され、認証コードとして認証コード用メモリ 21 に記憶される。このとき発生された認証コードは無線信号を利用して子機 24 に伝えられる。子機 24 では、認証コードを受け取ると、そのコードが符号化回路 26 に伝えられる。また、符号化回路には暗証コード用メモリ 25 に記憶された暗証コードも伝えられる。符号化回路 26 では認証コードと暗証コードを組み合わせて、あらかじめ決められた方法で変換する符号化を施し認証符号を生成する。親機から送られてくる認証コードと認証符号の生成方法を図 1 に示した第 1 の実施例と同様であるとする、子機 24 は、親機から送られてきた認証コード 01011011 と自らの記憶している、あるいは推測した暗証コード 1101100 と組み合わせ論理積を求め、この値 01001000 を認証符号として親機 60 に送信する。親機 60 では受信した認証符号を判定回路 22 に伝える。判定回路 22 では暗証コード用メモリ 19 および認証コード用メモリ 21 に記憶された暗証コードと認証コードをもとに、子機 24 より送られてきた認証符号が正しく符号化されているかを判定し、制御部 63 に出力する。親機 60 の暗証コード用メモリ 19 に記憶された暗証コードが図 1 に示した第 1 の実施例と同様に 11010001 とすると、正しく符号化された認証符号は、01010001 と成るため、子機から送られてきた認証符号 01001000 と一致せず、判定回路 22 は、制御部 63 に、認証符号の不一致を知らせる。制御部 63 は、認証符号の不一致が伝えられると、通話要求をしている子機は、不正な子機と判断し、通話を拒否する。また、カウンタ 61 に記憶されている、不正な子機と判断し通話を拒否した回数を 1 増やす。このとき、カウンタ 61 の値があらかじめ決められた値に達すると、制御部 63 は、全ての通話要求を拒否するモードになるように親機 60 を制御する。この状態に親機 60 がなると、正当な子機、不正な子機の如何に関わらずどのような子機からの通話要求にたいしても、親機 60 は無条件に通話を拒否し、不正な子機が繰り返し通話要求を行い認証符号を推測し、通話が許可されるのを防ぐ。また、上記した、通話拒否状態になった親機 60 は、リセットボタン

62 を押すことにより通常の動作状態に復帰する。リセットボタン 62 が、親機 60 の使用者によって押され、リセット信号が制御部 63 に伝えられると、制御部 63 は、カウンタ 61 の値を 0 に戻し、親機 60 を通常の動作状態で動作するように制御する。

【0041】次に第 7 の実施例について説明を行う。図 10 は本発明の第 7 の実施例を示す無線電話装置のブロック図である。上記した従来例、実施例と同様の効果、作用を有するものには、同一の図番を付し、説明を省略する。図 10 において、64 は 3 台の子機が登録可能な第 1 の無線装置としての親機であり、20 は認証コードを生成する認証コード発生部、21 は認証コード発生部 20 で作られた認証コードを記憶する認証コード記憶部としての認証コード用メモリ、22 は子機より送られてくる認証符号の判定を行う認証符号判定部としての判定回路、29 は親機 64 に登録された 3 台の子機の ID コードがそれぞれ記憶された ID コード記憶部としての ID コード用メモリ、30 は登録された 3 台の子機の各々の暗証コードが記憶された暗証コード記憶部としての暗証コード用メモリ、65 は登録された子機の ID を用いて不正に通話要求が行われた回数を該当する ID 毎にカウントし記憶する計数部としてのカウンタ、66 はカウンタ 65 の何れかの ID を持つ子機があらかじめ決められた値に達し該当する ID を持つ子機との通話が拒否状態になった状態から通常の状態に戻すための入力手段としてのリセットボタン、親機 64 全体の制御を行う制御部である。

【0042】また、32 は第 2 の無線装置としての子機であり、25 は暗証コードが記憶された暗証コード記憶部としての暗証コード用メモリ、26 は親機 64 から送られてきた認証コードと暗証コードを組み合わせて、あらかじめ決められた方法で変換する符号化を施し認証符号を生成する符号化回路、33 は子機 32 全体の制御を行う制御部である。

【0043】以上のように構成された無線電話装置についてその動作を説明する。まずはじめに子機 32 が正当な子機であるときの動作について説明を行う。子機 32 のキーパッド 13 の発呼ボタンが押されると、リンク確立要求が子機 32 より出力される。親機 64 が子機 32 から出されたリンク確立要求を受信すると、子機 32 に対し ID 要求を出力する。ID 要求を受信した子機 32 の制御部 33 は、ID コード用メモリ 12 より、ID コードを読みだし、親機 64 に出力する。子機 32 からの ID コードを受信した親機 64 の制御部 67 は、ID コード用メモリ 29 を検索し、どの子機からの通話要求であるかを調べ、カウンタ 65 より該当子機の ID を用いて不正に通話要求が行われ通話が拒否された回数を調べる。カウンタ 65 に記憶されている通話が拒否された回数があるあらかじめ決められた値に達している場合、制御部 67 は、無条件に通話を拒否するように親機 64 を

制御する。カウンタ65に記憶されている通話が拒否された回数があらかじめ決められた値に達していない場合、以後、図3に示した第2の実施例と同様に、認証コードと暗証コードを用いて子機の再確認が行われ通話モードに進む。

【0044】次に不正な子機からの通話要求があった場合の動作について説明を行う。本説明では、子機32は親機64が以前に通信した際にやり取りされたIDコード用メモリ29に記憶されたIDコードを盗聴し、盗聴したIDコードを使用している不正な子機であるとし、暗証コード用メモリに記憶されていて暗証コードは、親機64の暗証コードとことなる11001100が記憶されているものとする。子機32から通話要求を行う場合、使用者は、子機32のキーパッド13の発呼ボタンを押し、リンク確立要求を出力する。親機64は、子機32から出されたリンク確立要求を受信すると、上記した正当な子機からの通話要求を受信した場合と同様に、子機32に対しID要求を出力する。ID要求を受信した子機32の制御部33は、IDコード用メモリ12より、盗聴などによって得た親機64に登録された子機32の持つIDコードを読みだし、親機64に出力する。子機32からのIDコードを受信した親機64の制御部67は、IDコード用メモリ29を検索し、どの子機からの通話要求であるかを調べ、カウンタ65より該当子機のIDを用いて不正に通話要求が行われ通話が拒否された回数を調べる。カウンタ65に記憶されている通話が拒否された回数があらかじめ決められた値に達している場合、制御部67は、無条件に通話を拒否する用に親機64を制御する。カウンタ65に記憶されている通話が拒否された回数があらかじめ決められた値に達していない場合、認証コードと暗証コードを用いて子機の確認をおこなうシーケンスが開始され、図3に示した第2の実施例と同様に、親機64の認証コード発生部20で、ランダムなコードが生成され、認証コードとして認証コード用メモリ21に記憶される。このとき生成された認証コードは無線信号を利用して子機32に伝えられる。子機32では、認証コードを受け取ると、そのコードが符号化回路26に伝えられる。また、符号化回路26には暗証コード用メモリ25に記憶された暗証コードも伝えられる。符号化回路26では認証コードと暗証コードを組み合わせ、あらかじめ決められた方法で変換する符号化を施し認証符号を生成する。親機64から送られてくる認証コードと認証符号の生成方法を図3に示した第2の実施例と同様であるとする、子機32は、親機から送られてきた認証コード01011011と自らの記憶している、あるいは推測した暗証コード11001100と組み合わせ論理積を求め、この値01001000を認証符号として親機64に送信する。親機64では受信した認証符号を判定回路22に伝える。判定回路22では認証コード用メモリ21および暗証コード用

メモリ30に記憶された暗証コードと認証コードをもとに、子機32より送られてきた認証符号が正しく符号化されているかを判定し、制御部67に出力する。親機64の暗証コード用メモリ30に記憶された子機32が送ってきたIDコードを持つ子機の暗証コードが図3に示した第2の実施例と同様に11010001とすると、正しく符号化された認証符号は、01010001と成るため、子機から送られてきた認証符号01001000と一致せず、判定回路22は、制御部67に、認証符号の不一致を知らせる。制御部67は、認証符号の不一致が伝えられると、通話要求をしている子機は、不正な子機と判断し、通話を拒否する。また、該当するIDコードを有する子機が不正な子機と判断され通話が拒否された回数を記憶しているカウンタ65の該当するカウンタの値を1増やす。このとき、カウンタ65の値があらかじめ決められた値に達すると、制御部67は、該当するIDコードを用いて通話要求を行ってきた子機からの通話要求を拒否するモードになるように親機64を制御する。この状態に親機64がなると、該当するIDコードを有する正当な子機、不正な子機の如何に関わらず該当するIDコードを用いて通話要求をおこなってきたどのような子機からの通話要求にたいしても、親機64は無条件に通話を拒否し、IDコードを盗聴するなどして通話要求を行ってきた不正な子機が繰り返し通話要求を行い認証符号を推測し、通話が許可されるのを防ぐ。また、上記した、通話拒否状態になった親機64は、リセットボタン66を押すことにより通常の動作状態に復帰する。なお、リセットボタン66は、登録された子機毎に用意されているかもしれない。リセットボタン66が、親機64の使用者によって押され、リセット信号が制御部67に伝えられると、制御部67は、カウンタ65の全ての値、あるいは、該当する子機の値を0に戻し、親機64を通常の動作状態で動作するように制御する。

【0045】図11は本発明の第8の実施例を示す無線電話装置のブロック図である。図11において、68は第1の無線装置としての親機であり、20は認証コードを生成する認証コード発生部、21は認証コード発生部20で作られた認証コードを記憶する認証コード記憶部としての認証コード用メモリ、22は子機より送られてくる認証符号の判定を行う認証符号判定部としての判定回路、69は複数の暗証コードが記憶された暗証コード記憶部としての暗証コード用メモリ、70は認証コードを符号化の際にどの暗証コードを用いるかをランダムに決定する暗証コード選択部、71は親機68全体の制御を行う制御部である。

【0046】また、72は第2の無線装置としての子機であり、26は親機68から送られてきた認証コードと暗証コードを組み合わせ、あらかじめ決められた方法で変換する符号化を施し認証符号を生成する符号化回

路、73は複数の暗証コードが記憶された暗証コード記憶部としての暗証コード用メモリ、74は子機72全体の制御を行う制御部である。

【0047】図12は、子機72から親機68への通話要求があったときの信号のやり取りのシーケンスの例を示す図である。以上のように構成された無線電話装置についてその動作を説明する。子機72のキーパッド13の発呼ボタンが押されると、リンク確立要求が子機72より出力される。親機68が子機72から出されたリンク確立要求を受信すると、認証コードと暗証コードを用いて子機の確認が行われる。親機68の制御部71は、認証コード発生部20を起動し、認証コード発生部20でランダムなコードが生成され、認証コードとして認証コード用メモリ21に記憶される。また、制御部71は暗証コード選択部70を起動し、暗証コード選択部70は、認証コードを符号化する際にどの暗証コードを用いるかをランダムに決定し制御部71に伝える。制御部71は、認証コード発生部20で作られた認証コードと、暗証コード選択部70にて決定された暗証コードを指定する信号をデータ処理部4に出力する。データ処理部4は、暗証コードの選択番号と認証コードを組み合わせ無線部2に出力し、無線部より、無線信号が出力される。暗証コードの選択番号と認証コードを組み合わせた無線信号が、子機72の無線部9にて受信されると、暗証コードの選択番号と認証コードを組み合わせた無線信号が復調され、データ処理部11に伝えられる。データ処理部11は、暗証コードの選択番号と認証コードを制御部74に伝える。制御部74は、受け取った認証コードを符号化回路26に伝え、また、選択番号によって指定された暗証コードを暗証コード用メモリ73より読み込み、同様に符号化回路26に伝える。符号化回路26では認証コードと暗証コードを組み合わせ、あらかじめ決められた方法で変換する符号化を施し認証符号を生成し、制御部74に出力する。制御部74は、データ処理部11を符号化回路26より受け取った認証符号を出力するように制御し、データ処理部11より無線部9に認証符号が出力され、無線部9より無線信号として出力される。認証符号の無線信号が、親機68の無線部2にて受信されると、認証符号の無線信号が復調され、データ処理部4に伝えられる。データ処理部4は、認証符号を制御部71に伝える。制御部71は、受け取った認証符号を判定回路22に伝え、また、兼ね合い選択番号によって指定された暗証コードと認証コード用メモリ21に記憶された認証コードを読みだし、同様に判定回路22に伝える。判定回路22は、子機から送られてきた認証符号が、指定された暗証コードと認証コードを組み合わせ、あらかじめ決められた符号化がなされているかを判定し、制御部71に出力する。制御部71では、受信した認証符号が正しく符号化されている場合は、正当な子機からの通信であると判断し、親機子機間のリンクを確

立し、通話チャネルの指定などのシーケンスを経て、親機子機間が通話状態にするように制御を行う。また、受信した認証符号正しくなかった場合は、不当な子機からの通信であると判断し、通信を拒否する。

【0048】また、本実施例の発展的応用として、上記した認証コードを用いた子機の確認を繰り返し行い、より確実に不正使用を防ぐ方法が考えられる。この場合、上記した一回目の認証コードによる子機の確認を行った後、再度、1回目と同様に、新たに認証コードを生成し、また、暗証コードを選択して子機に送り、子機からの新たな認証符号を受け取り再確認を行う。

【0049】次に図12を用いて、本発明の一実施例である図11に示す無線電話装置の親機子機間での通話要求からリンク確立までにやり取りされる信号の流れを説明する。なお、図11の例では、上記した本実施例の発展的応用である繰り返し認証コードを用いた子機の確認を行う例を示す。図に示すように子機では、使用者が発呼ボタンを押して電話をかけようとする、まず、親機にリンクの確立を要求するリンク確立要求が出力される。リンク確立要求を受け取った親機は、暗証コード選択部によって決定された暗証コードの選択番号と認証コード発生部で生成された認証コードを子機に出力する。子機は、送られてきた認証コードと選択番号によって指定された暗証コードを組み合わせた符号化回路で符号化し、親機に出力する。親機では、子機より送られてきた認証符号が正しく符号化されているかを判定し、正しく符号化されている場合は、二度目の認証コードによる確認を開始し、上記した一度目の確認と同様に、新たに暗証コード選択部によって決定された暗証コードの選択番号と認証コード発生部で生成された認証コードを子機に出力する。子機は、送られてきた新たな認証コードと選択番号によって指定された暗証コードを組み合わせ符号化回路で符号化し、親機に出力する。親機は、子機より送られてきた二回目の認証符号が正しく符号化されているかを判定し、正しく符号化されている場合は、リンクを確立し、通話チャネルの指定などを経て通話モードにはいる。また、子機から送られてきた認証符号が正しく符号化されていない場合は、その時点で通信が拒否され、リンクは確立されない。なお、本実施例では、親機子機それぞれの暗証コード用メモリに記憶された第1の暗証コードを11010001、第3の暗証コードを10101101、また、一回目の確認の際に指定された暗証コードが第1の暗証コードであり、そのときの認証コードが01011011、二回目の確認の際に指定された暗証コードが第3の暗証コードであり、そのときの認証コードが10011010、加えて符号化の一例として認証コードと暗証コードの論理積をとって認証符号とする例を示している。図12に示すように、親機から送られてくる認証コードが01011011、選択番号によって指定された暗証コードが11010001であ

る場合、正しく符号化された認証符号は、01010001となり、子機はこの01010001を認証符号として親機に送信している。同様に、親機から送られてくる認証コードが10011010、選択番号によって指定された暗証コードが10101101である場合、正しく符号化された認証符号は、10001000となり、子機は二度目の確認では10001000を認証符号として親機に送信している。

【0050】図13は本発明の第9の実施例を示す無線電話装置のブロック図である。図13において、75は第1の無線装置としての親機であり、20は認証コードを生成する認証コード発生部、21は認証コード発生部20で作られた認証コードを記憶する認証コード記憶部としての認証コード用メモリ、69は複数の暗証コードが記憶された暗証コード記憶部としての暗証コード用メモリ、76は認証コードを符号化する際にどの暗証コードを用いるかをランダムに決定し複数の暗証コードを選択する暗証コード選択部、77は子機より送られてくる複数の認証符号の判定をそれぞれ行う認証符号判定部としての判定回路、78は親機75全体の制御を行う制御部である。

【0051】また、79は第2の無線装置としての子機であり、73は複数の暗証コードが記憶された暗証コード記憶部としての暗証コード用メモリ、80は親機75から送られてきた認証コードと指定された暗証コードを組み合わせ、あらかじめ決められた方法で変換する符号化を施し認証符号を生成する符号化回路、81は子機79全体の制御を行う制御部である。

【0052】図14は、子機79から親機75への通話要求があったときの信号のやり取りのシーケンスの例を示す図である。以上のように構成された無線電話装置についてその動作を説明する。子機79のキーパッド13の発呼ボタンが押されると、リンク確立要求が子機79より出力される。親機75が子機79から出されたリンク確立要求を受信すると、認証コードと暗証コードを用いて子機の確認が行われる。親機75の制御部78は、認証コード発生部20を起動し、認証コード発生部20でランダムなコードが生成され、認証コードとして認証コード用メモリ21に記憶される。また、制御部78は暗証コード選択部76を起動し、暗証コード選択部76は、認証コードを符号化する際に用いる複数の暗証コードをランダムに決定し制御部78に伝える。制御部78は、認証コード発生部20で作られた認証コードと、暗証コード選択部76にて決定され複数の暗証コードを指定する信号をデータ処理部4に出力する。データ処理部4は、複数の暗証コードの選択番号と認証コードを組み合わせ無線部2に出力し、無線部より、無線信号が出力される。複数の暗証コードの選択番号と認証コードを組み合わせ無線信号が、子機79の無線部9にて受信されると、複数の暗証コードの選択番号と認証コードを組

み合わせた無線信号が復調され、データ処理部11に伝えられる。データ処理部11は、複数の暗証コードの選択番号と認証コードを制御部81に伝える。制御部81は、受け取った認証コードを符号化回路80に伝え、また、複数の選択番号によって指定された全ての暗証コードを暗証コード用メモリ73より読み込み、同様に符号化回路80に伝える。符号化回路80では受け取った暗証コードと認証コードを順次組み合わせ、あらかじめ決められた符号化を施し指定された暗証コード毎に認証符号を生成し、制御部81に出力する。制御部81は、データ処理部11を符号化回路80より受け取った全ての認証符号を順次出力するように制御し、データ処理部11より無線部9に認証符号が出力され、無線部9より無線信号として出力される。認証符号の無線信号が、親機75の無線部2にて受信されると、認証符号の無線信号が復調され、データ処理部4に伝えられる。データ処理部4は、全ての認証符号を制御部78に伝える。制御部78は、受け取った全ての認証符号を順次判定回路77に伝え、また、先に読み込んだ選択番号によって指定された全ての暗証コードと認証コード用メモリ21に記憶された認証コードを読みだし、同様に判定回路77に伝える。判定回路77は、子機から送られてきた全ての認証符号が、指定された暗証コードと認証コードを組み合わせ、あらかじめ決められた符号化がなれているかを判定し、制御部78に出力する。制御部78では、受信した全ての認証符号が正しく符号化されている場合は、正当な子機からの通信であると判断し、親機子機間のリンクを確立し、通話チャネルの指定などのシーケンスを経て、親機子機間が通話状態にするように制御を行う。また、受信した認証符号正しくなかった場合は、不当な子機からの通信であると判断し、通信を拒否する。

【0053】また、本実施例の発展的応用として、上記した認証コードを用いた子機の確認を繰り返し行い、より確実に不正使用を防ぐ方法が考えられる。この場合、上記した一回目の認証コードによる子機の確認を行った後、再度、1回目と同様に、新たに認証コードを生成し、また、複数の暗証コードを選択して子機に送り、子機からの新たな認証符号を受け取り再確認を行う。

【0054】次に図14を用いて、本発明の一実施例である図13に示す無線電話装置の親機子機間での通話要求からリンク確立までにやり取りされる信号の流れを説明する。なお、本例では、親機の暗証コード選択部にて2つの暗証コードが指定された例を示す。図に示すように子機では、使用者が発呼ボタンを押して電話をかけようとすると、まず、親機にリンクの確立を要求するリンク確立要求が出力される。リンク確立要求を受け取った親機は、暗証コード選択部によって決定された2つの暗証コードの選択番号と認証コード発生部で生成された認証コードを子機に出力する。子機は、送られてきた認証コードと選択番号によって指定された2つの暗証コード

をそれぞれ組み合わせ符号化回路で符号化し、親機に生成された2つの認証符号を順次出力する。親機では、子機より送られてきた2つの認証符号が正しく符号化されているかを判定し、正しく符号化されている場合は、リンクを確立し、通話チャネルの指定などを経て通話モードにはいる。また、子機から送られてきた認証符号が正しく符号化されていない場合は、その時点で通信が拒否され、リンクは確立されない。なお、本実施例では、親機子機それぞれの暗証コード用メモリに記憶された第1の暗証コードを11010001、第3の暗証コードを10101101、また、暗証コード選択部によって指定された2つの暗証コードが第1の暗証コードと第3の暗証コードであり、認証コードが01011011、加えて符号化の一例として認証コードと暗証コードの論理積をとって認証符号とする例を示している。図14に示すように、親機から送られてくる認証コードが01011011、選択番号によって指定された暗証コードが11010001である場合、正しく符号化された認証符号は、01010001となり、子機はこの01010001を1つ目の認証符号として親機に送信している。同様に、選択番号によって指定された暗証コードが10101101である場合、正しく符号化された認証符号は、00001001となり、子機は00001001を2つめの認証符号として親機に送信している。

【0055】図15は本発明の第10の実施例を示す無線電話装置のブロック図である。図15において、82は第1の無線装置としての親機であり、20は認証コードを生成する認証コード発生部、21は認証コード発生部20で作られた認証コードを記憶する認証コード記憶部としての認証コード用メモリ、69は複数の暗証コードが記憶された暗証コード記憶部としての暗証コード用メモリ、76は認証コードを符号化する際にどの暗証コードを用いるかをランダムに決定し複数の暗証コードを選択する暗証コード選択部、83は子機より送られてくる認証符号の判定を行う認証符号判定部としての複合判定回路、84は親機82全体の制御を行う制御部である。

【0056】また、85は第2の無線装置としての子機であり、73は複数の暗証コードが記憶された暗証コード記憶部としての暗証コード用メモリ、86は親機82から送られてきた認証コードと指定された全ての暗証コードを組み合わせ、あらかじめ決められた方法で変換する符号化を施し認証符号を生成する複合符号化回路、87は子機85全体の制御を行う制御部である。

【0057】図15は、子機85から親機82への通話要求があったときの信号のやり取りのシーケンスの例を示す図である。以上のように構成された無線電話装置についてその動作を説明する。子機85のキヤパッド13の発呼ボタンが押されると、リンク確立要求が子機85より出力される。親機82が子機85から出されたリン

ク確立要求を受信すると、認証コードと暗証コードを用いて子機の確認が行われる。親機82の制御部84は、認証コード発生部20を起動し、認証コード発生部20でランダムなコードが生成され、認証コードとして認証コード用メモリ21に記憶される。また、制御部84は暗証コード選択部76を起動し、暗証コード選択部76は、認証コードを符号化する際に用いる複数の暗証コードをランダムに決定し制御部84に伝える。制御部84は、認証コード発生部20で作られた認証コードと、暗証コード選択部76にて決定された複数の暗証コードを指定する信号をデータ処理部4に出力する。データ処理部4は、複数の暗証コードの選択番号と認証コードを組み合わせ無線部2に出力し、無線部より、無線信号が出力される。複数の暗証コードの選択番号と認証コードを組み合わせ無線信号が、子機85の無線部9にて受信されると、複数の暗証コードの選択番号と認証コードを組み合わせ無線信号が復調され、データ処理部11に伝えられる。データ処理部11は、複数の暗証コードの選択番号と認証コードを制御部87に伝える。制御部87は、受け取った認証コードを複合符号化回路86に伝え、また、複数の選択番号によって指定された全ての暗証コードを暗証コード用メモリ73より読み込み、同様に複合符号化回路86に伝える。複合符号化回路86では受け取った暗証コードと認証コードをすべて組み合わせ、あらかじめ決められた符号化を施し認証符号を生成し、制御部87に出力する。制御部87は、データ処理部11を複合符号化回路86より受け取った認証符号を出力するように制御し、データ処理部11より無線部9に認証符号が出力され、無線部9より無線信号として出力される。認証符号の無線信号が、親機82の無線部2にて受信されると、認証符号の無線信号が復調され、データ処理部4に伝えられる。データ処理部4は、認証符号を制御部84に伝える。制御部84は、受け取った認証符号を複合判定回路83に伝え、また、先に読み込んだ選択番号によって指定された全ての暗証コードと認証コード用メモリ21に記憶された認証コードを読みだし、同様に複合判定回路83に伝える。複合判定回路83は、子機から送られてきた認証符号が、指定された全ての暗証コードと認証コードを組み合わせ、あらかじめ決められた符号化がなされているかを判定し、制御部84に出力する。制御部84では、受信した認証符号が正しく符号化されている場合は、正当な子機からの通信であると判断し、親機子機間のリンクを確立し、通話チャネルの指定などのシーケンスを経て、親機子機間が通話状態になるように制御を行う。また、受信した認証符号正しくなかった場合は、不当な子機からの通信であると判断し、通信を拒否する。

【0058】また、本実施例の発展的応用として、上記した認証コードを用いた子機の確認を繰り返し行い、より確実に不正使用を防ぐ方法が考えられる。この場合、

上記した一回目の認証コードによる子機の確認を行った後、再度、1回目と同様に新たに認証コードを生成し、また、複数の暗証コードを選択して子機に送り、子機からの新たな認証符号を受け取り再確認を行う。次に図16を用いて、本発明の一実施例である図15に示す無線電話装置の親機子機間での通話要求からリンク確立までにやり取りされる信号の流れを説明する。なお、本例では、親機の暗証コード選択部にて2つの暗証コードが指定された例を示す。図に示すように子機では、使用者が発呼ボタンを押して電話をかけようとする、まず、親機にリンクの確立を要求するリンク確立要求が出力される。リンク確立要求を受け取った親機は、暗証コード選択部によって決定された2つの暗証コードの選択番号と認証コード発生部で生成された認証コードを子機に出力する。子機は、送られてきた認証コードと選択番号によって指定された2つの暗証コードを全て組み合わせ符号化回路で符号化し、親機に生成された認証符号を出力する。親機では、子機より送られてきた認証符号が正しく符号化されているかを判定し、正しく符号化されている場合は、リンクを確立し、通話チャンネルの指定などを経て通話モードにはいる。また、子機から送られてきた認証符号が正しく符号化されていない場合は、その時点で通信が拒否され、リンクは確立されない。なお、本実施例では、親機子機それぞれの暗証コード用メモリに記憶された第1の暗証コードを11010001、第3の暗証コードを10101101、また、暗証コード選択部によって指定された2つの暗証コードが第1の暗証コードと第3の暗証コードであり、認証コードが01011011、加えて符号化の一例として認証コードと指定された2つの暗証コードの3つの排他的論理和をとって認証符号とする例を示している。図16に示すように、親機から送られてくる認証コードが01011011、選択番号によって指定された暗証コードが11010001と10101101である場合、3つを組み合わせ正しく符号化された認証符号は、00100111となり、子機はこの00100111を認証符号として親機に送信している。

【0059】上記の第1の実施例～第10の実施例の動作により、子機が通信要求の際に送信するIDコードや認証符号が盗聴されても、不正使用される危険性を少なくできる。

【0060】以上、本発明の実施例では、親機と子機、すなわち、家庭用のコードレス電話への応用を例として述べたが、本発明は、セルラー電話や、家庭用のコードレス電話と小ゾーンシステムのセルラー電話が組み合わせられた第2世代コードレス電話などに於いても利用が可能であることはもちろんである。

【0061】

【発明の効果】以上のように本発明によれば、第2の無線装置の確認のために、IDコードによる確認に加え、

第1の無線装置と第2の無線装置の双方に記憶された暗証コードを利用し、第2の無線装置からの通信要求毎に、第1の無線装置において任意に生成され送信された認証コードを、第2の無線装置側で暗証コードと組み合わせ予め決められた方法で符号化した認証符号として第1の無線装置に送信し、第1の無線装置において、送信した認証コードと記憶している暗証コードとに基づいて、受信した認証符号が正しく符号化されていると判断し、第2の無線装置を確認した場合に、この第2の無線装置に対して通話を許可する。

【0062】そのため、第2の無線装置からの通信要求の際に、第1の無線装置は第2の無線装置の確認を行うための暗証コードを送る必要がなく、前記の通信要求の度にランダムに作られる第2の無線装置確認用の認証コードとそれとともなって変化する認証符号が盗聴されても、暗証コードが知られる可能性が少なく、不正使用の危険性が大幅に改善できる。また、暗証コードを定期的に変更したり複数の暗証コードや認証コードを組み合わせることによって、不正使用に対する安全性をさらに高めることができる。

【図面の簡単な説明】

【図1】本発明の第1の実施例の無線電話装置の構成図

【図2】同実施例で通話を行うときのシーケンス図

【図3】本発明の第2の実施例の無線電話装置の構成図

【図4】同実施例で通話を行うときのシーケンス図

【図5】本発明の第3の実施例の無線電話装置の構成図

【図6】本発明の第4の実施例の無線電話装置の構成図

【図7】本発明の第5の実施例の無線電話装置の構成図

【図8】同実施例で通話を行うときのシーケンス図

【図9】本発明の第6の実施例の無線電話装置の構成図

【図10】本発明の第7の実施例の無線電話装置の構成図

【図11】本発明の第8の実施例の無線電話装置の構成図

【図12】同実施例で通話を行うときのシーケンス図

【図13】本発明の第9の実施例の無線電話装置の構成図

【図14】同実施例で通話を行うときのシーケンス図

【図15】本発明の第10の実施例の無線電話装置の構成図

【図16】同実施例で通話を行うときのシーケンス図

【図17】従来の無線電話装置の構成図

【図18】同従来例で通話を行うときのシーケンス図

【符号の説明】

18, 28, 34, 44, 50, 60, 64, 68, 7

5, 82 親機

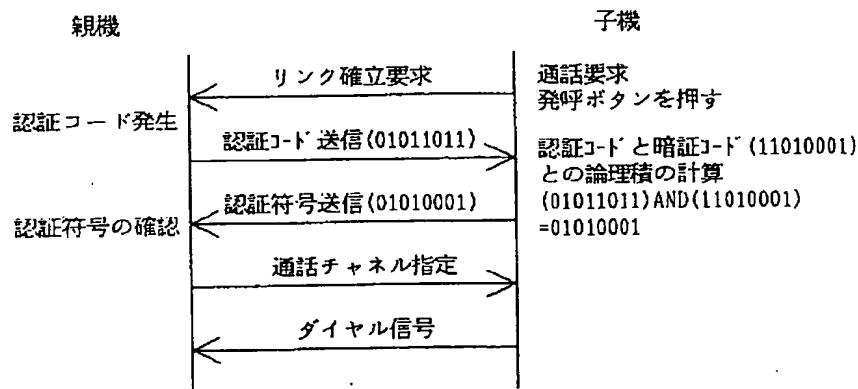
19, 30, 35, 69 暗証コード用メモリ(親機側)

20 認証コード発生部

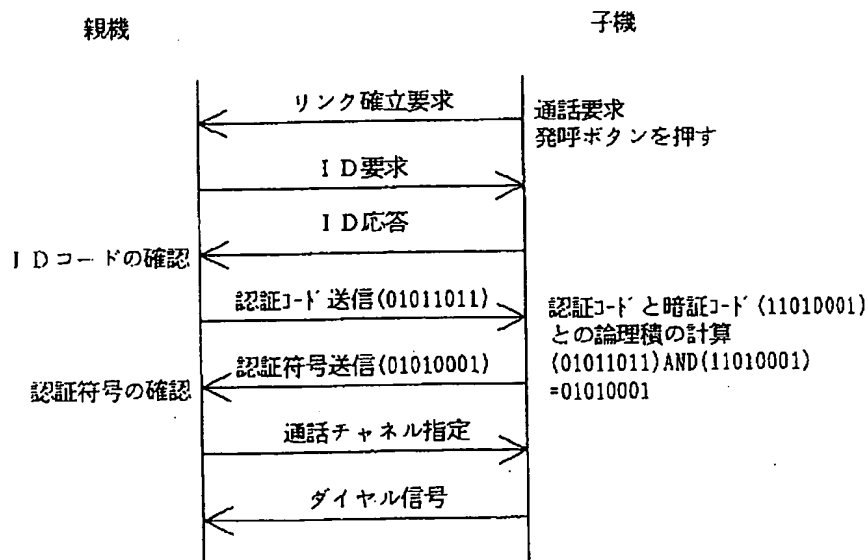
21 認証コード用メモリ

22, 77	判定回路	47	制御部
24, 32, 40, 48, 55, 72, 79, 85		52	送信部
子機		53	暗証コード暗号化器
25, 41, 73	暗証コード用メモリ (子機側)	56	受信部
26, 80	符号化回路	58	暗証コード復号器
29	IDコード用メモリ	61, 65	カウンタ
36	暗証コード発生部	62, 66	リセットボタン
37	インターフェイス部 (親機側)	70, 76	暗証コード選択部
38, 45	接続検知部	83	複合判定回路
42	インターフェイス部 (子機側)	86	複合符号化回路

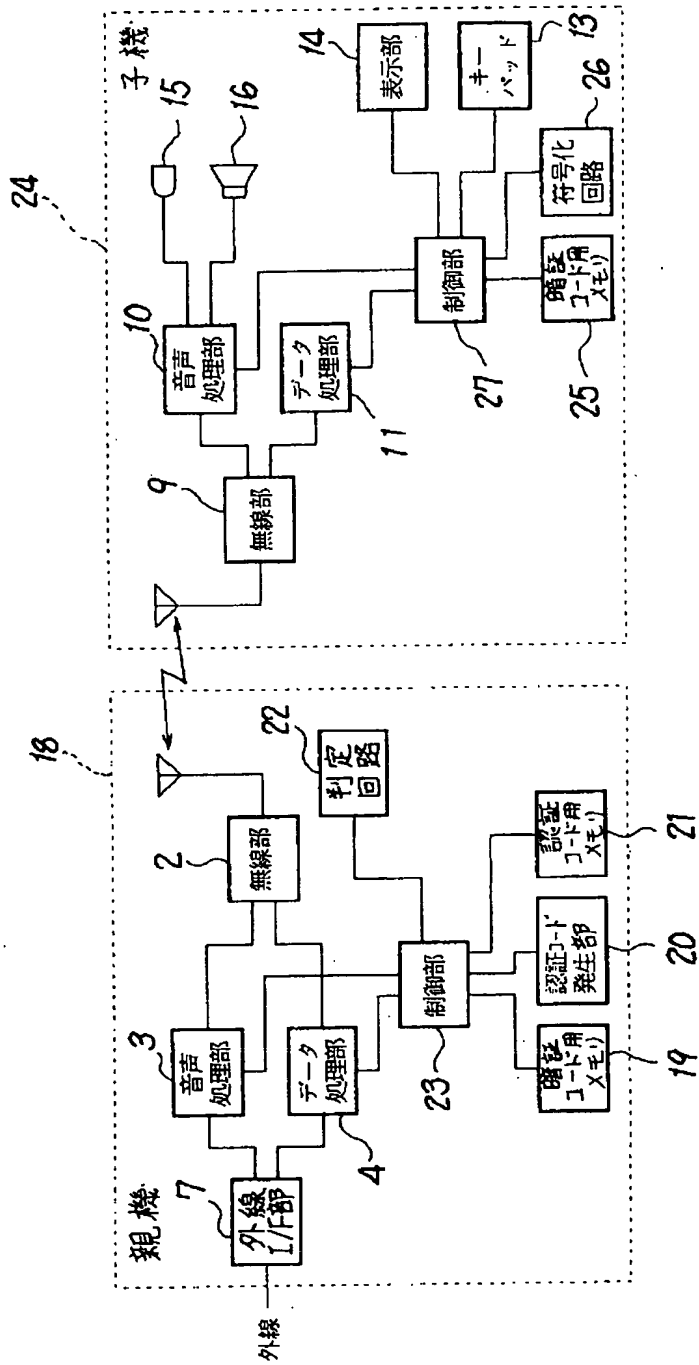
【図2】



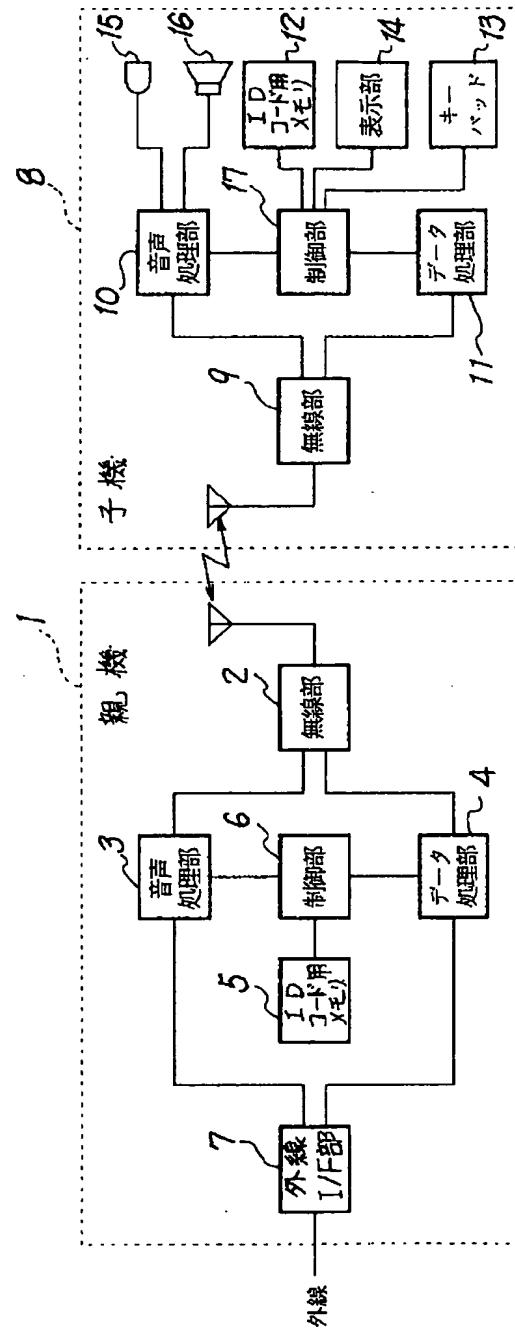
【図4】



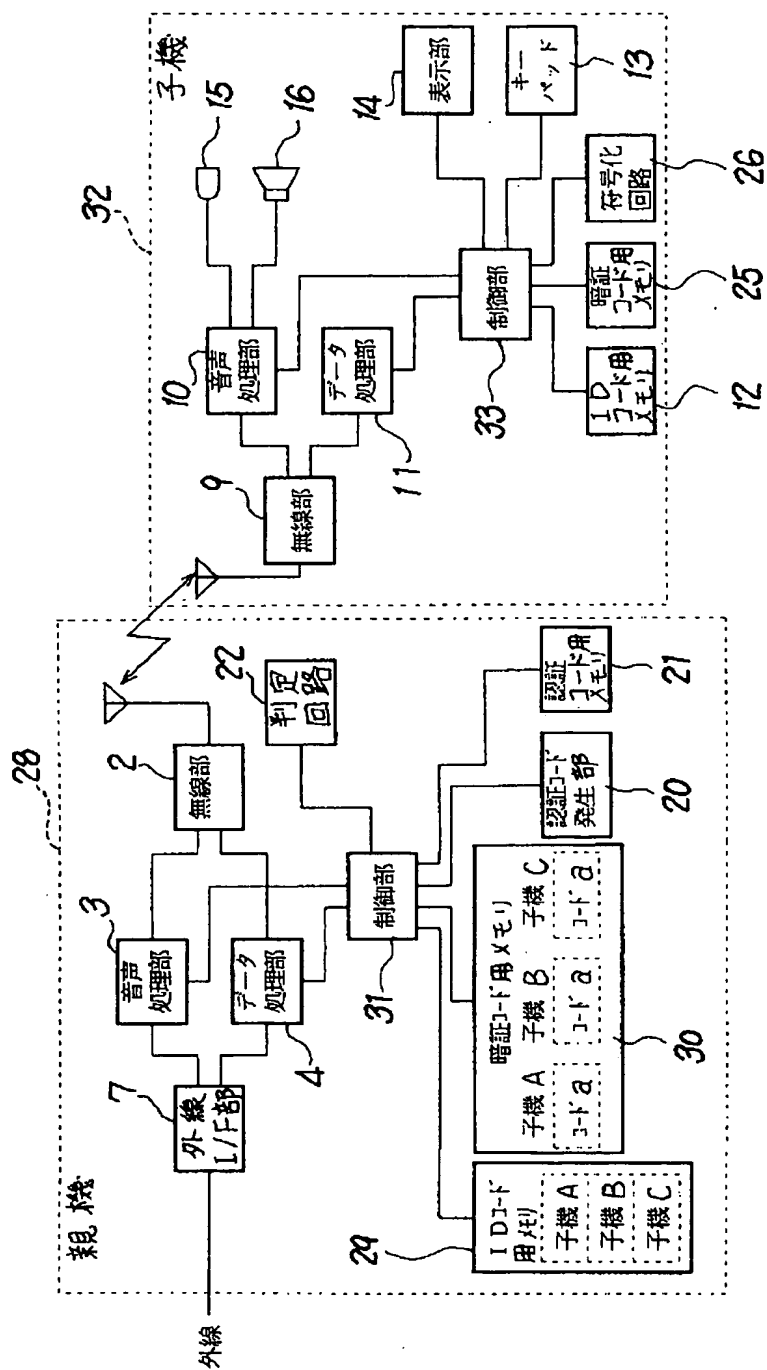
【図 1】



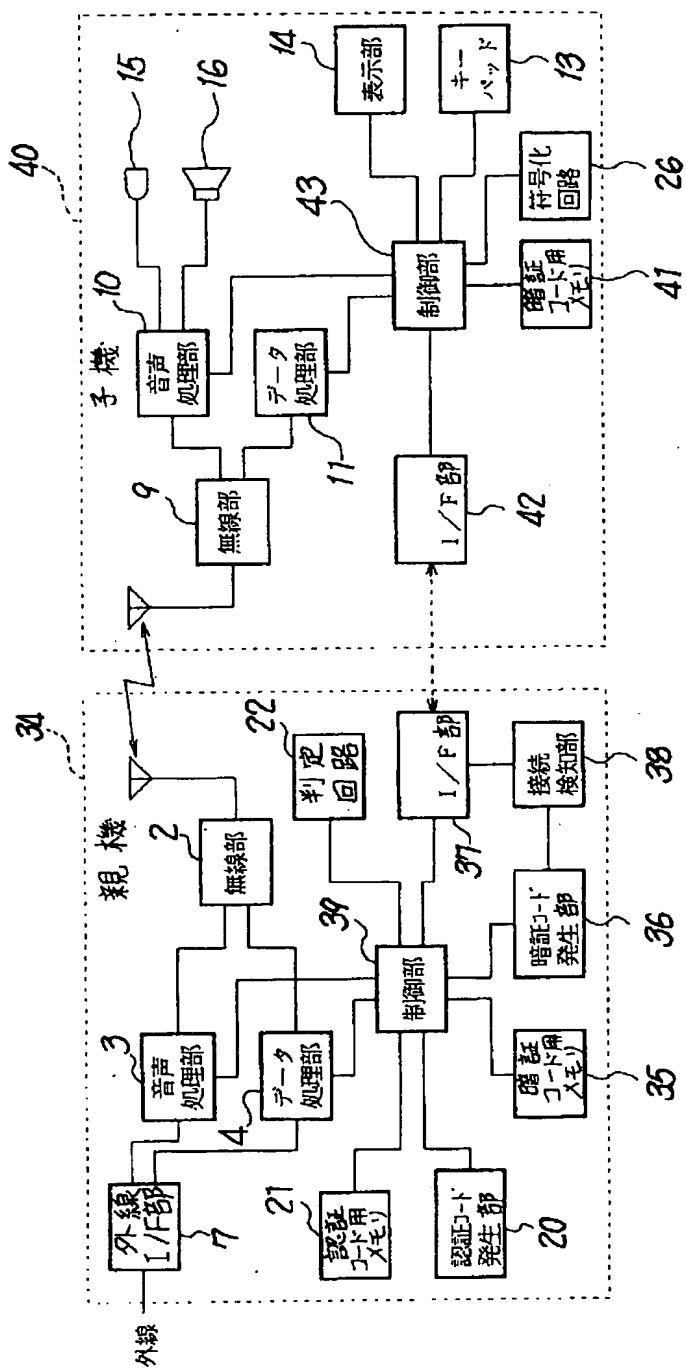
【図 17】



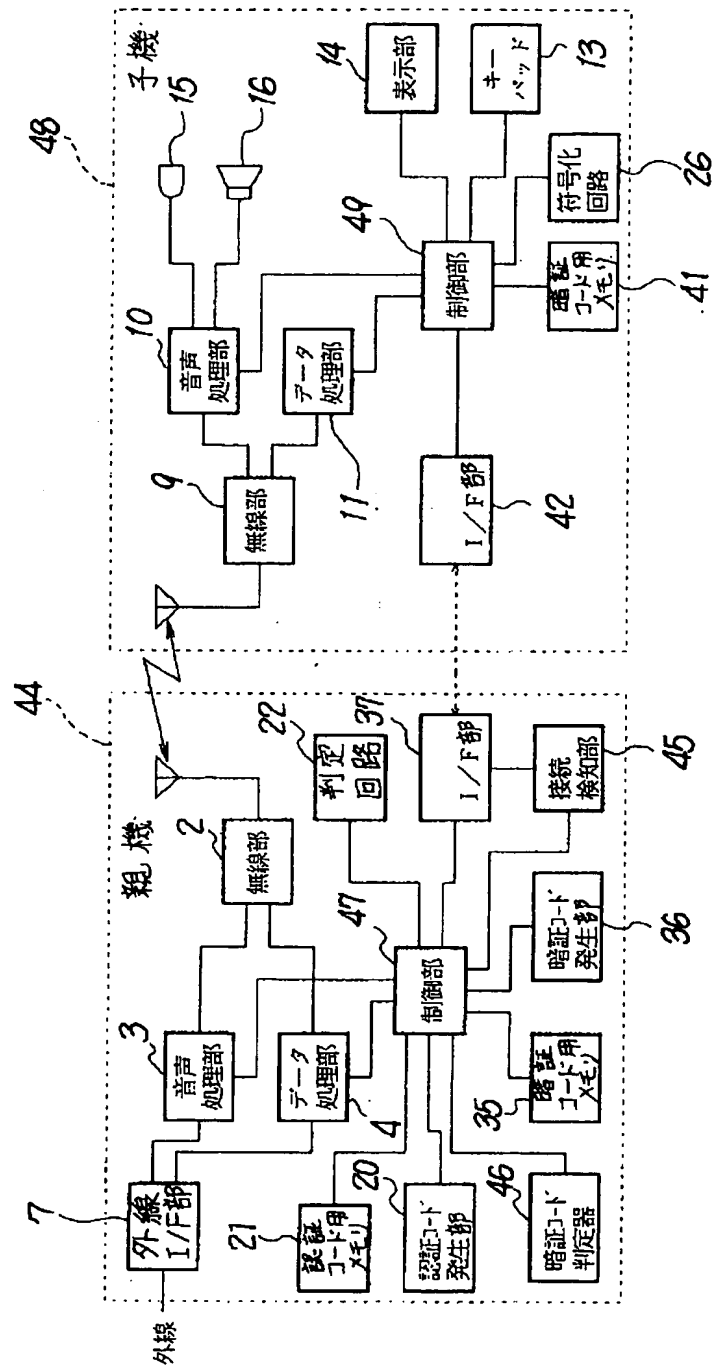
【図 3】



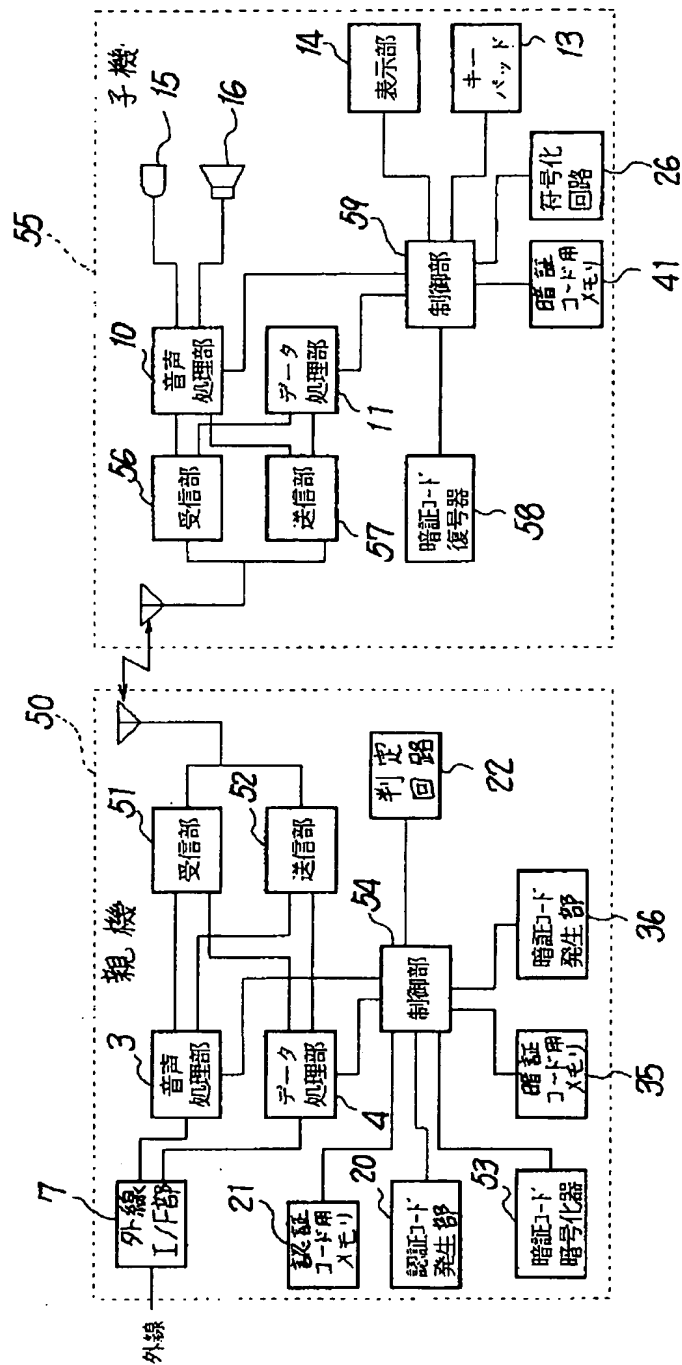
【図 5】



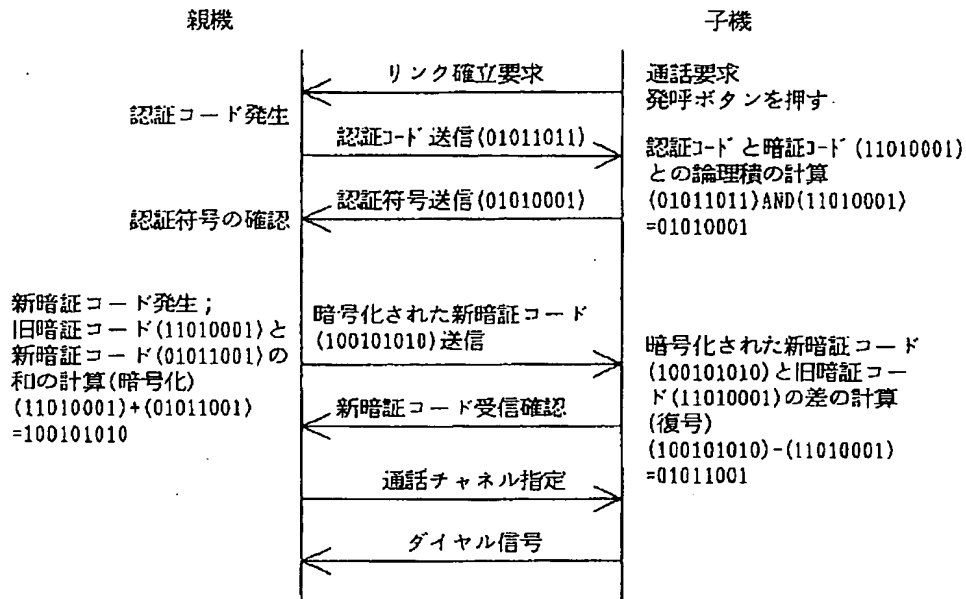
【図6】



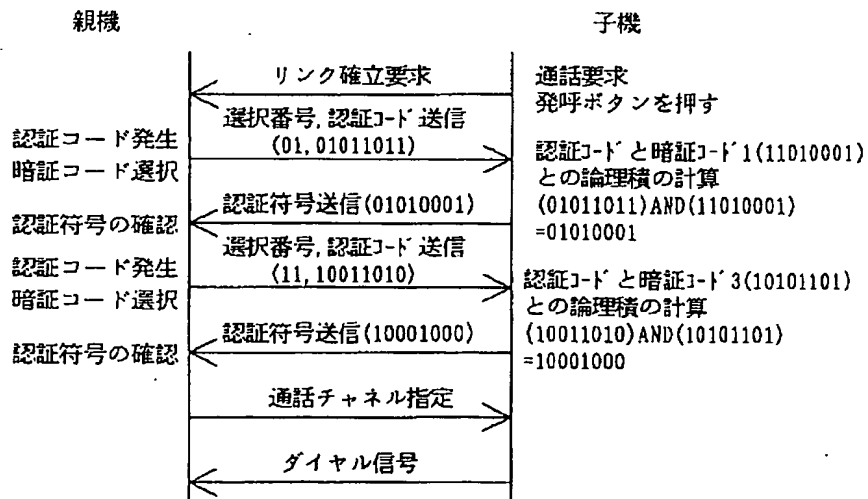
【図 7】



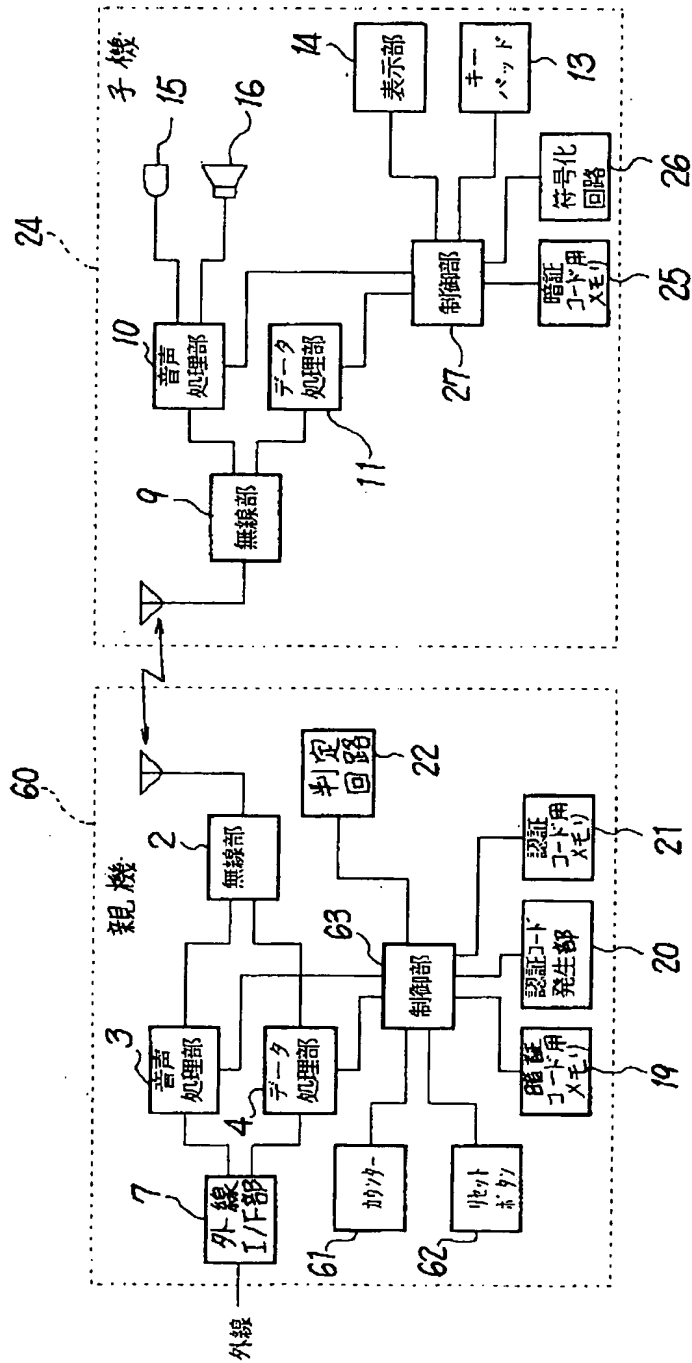
【図 8】



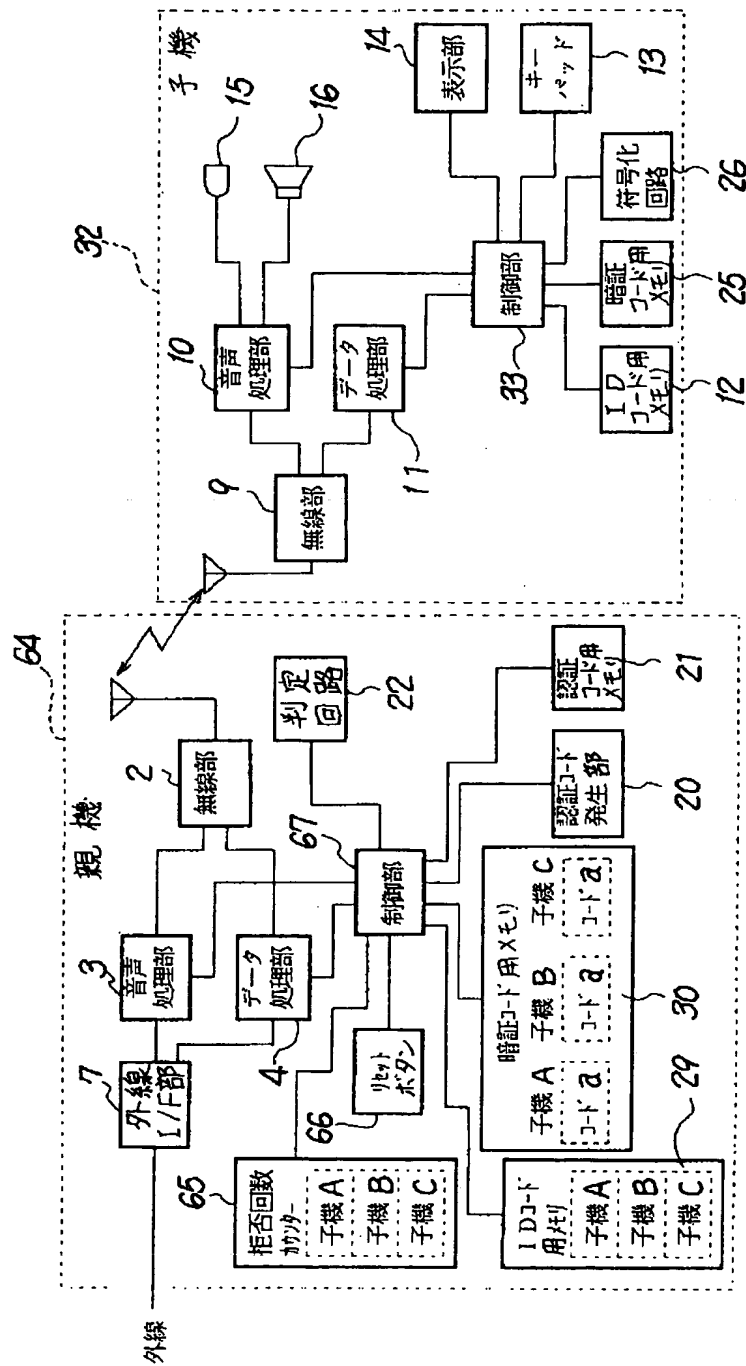
【図 12】



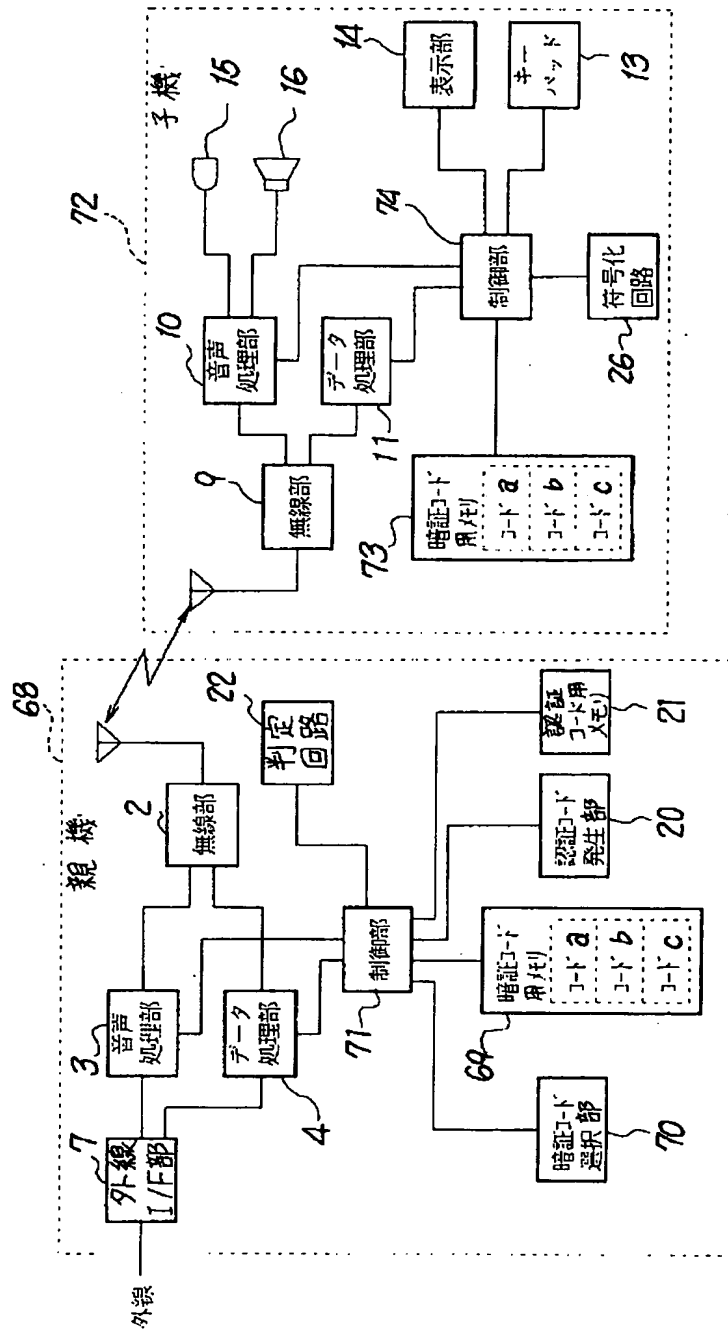
【図 9】



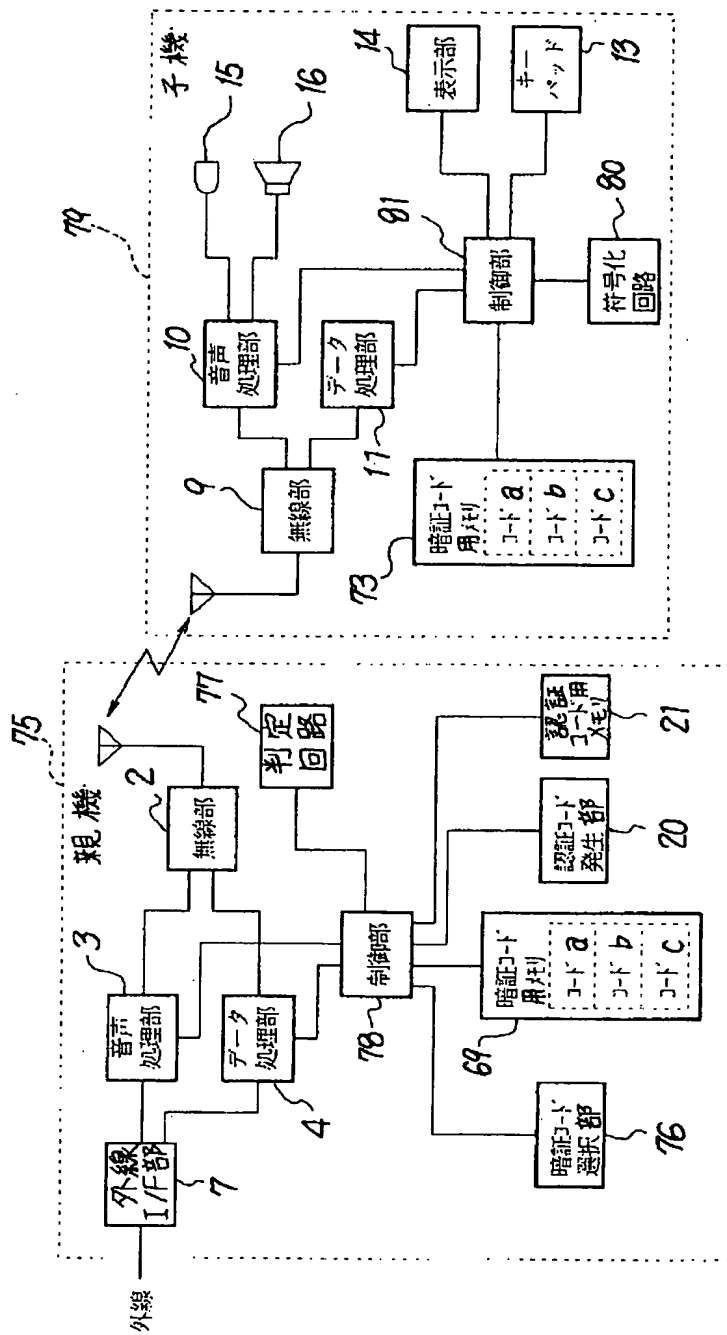
【図10】



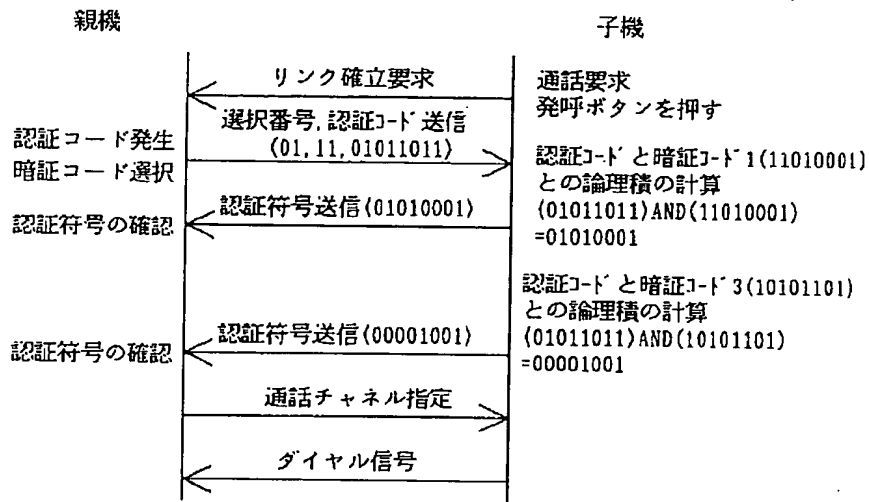
【図11】



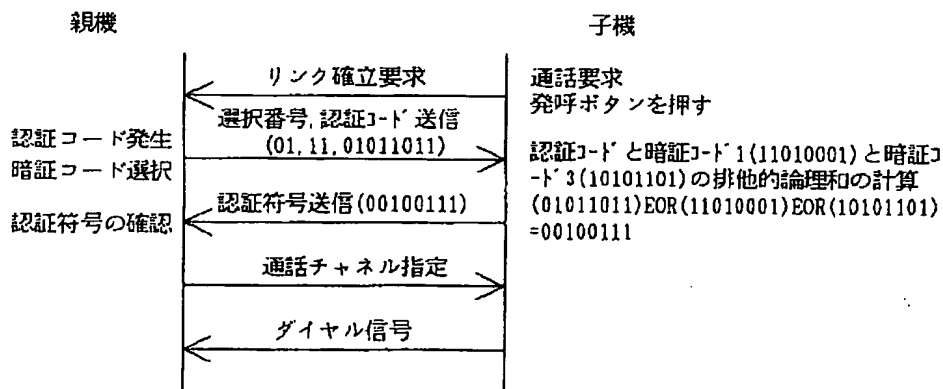
【図 13】



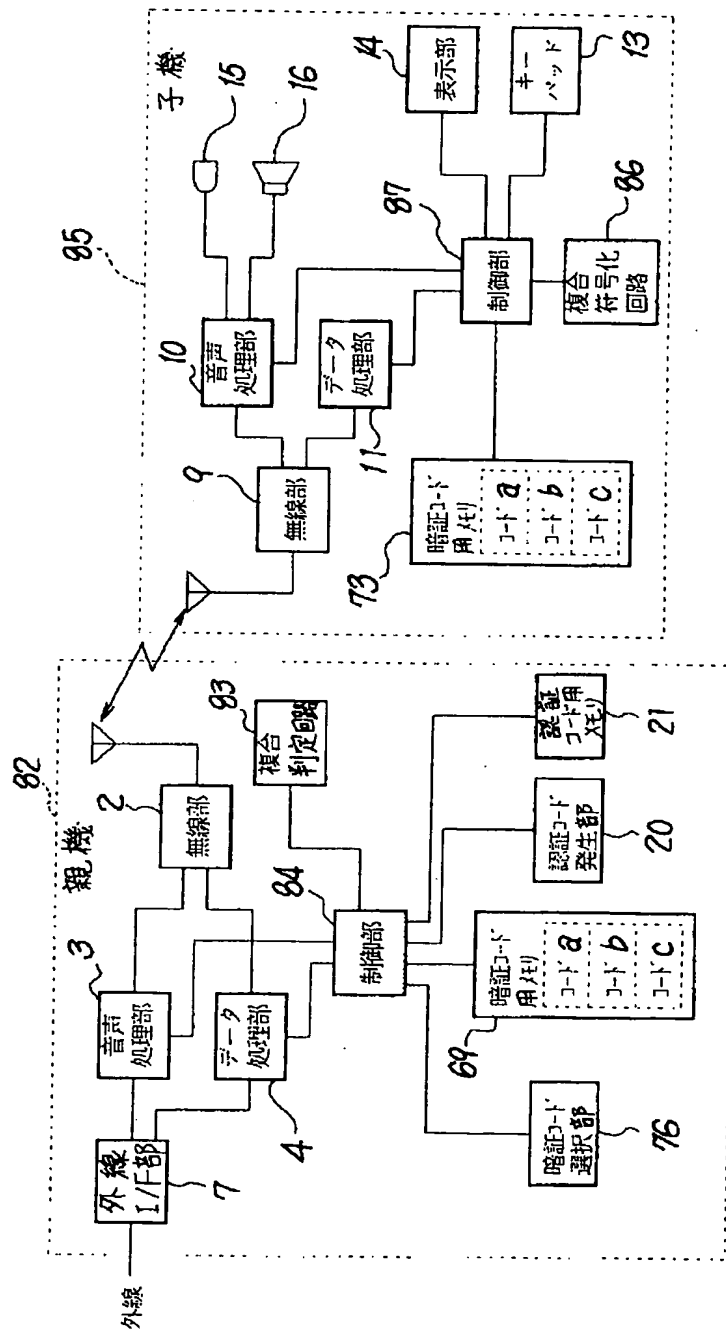
【図 1 4】



【図 1 6】



【図15】



【図18】

